

Abou Bekr Belkaid University

Tlemcen Algeria



جامعة أبي بكر بلقايد

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA  
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH  
FACULTY OF SCIENCES  
DEPARTMENT OF COMPUTER SCIENCES

# DOCTORAL THESIS

*A thesis submitted for the award of the degree of*

*Doctor of Philosophy*

*In: COMPUTER SCIENCE*

*Speciality: Networks and Distributed Systems*

*by*

**Hafida SAIDI**

---

## Privacy preserving IoT-based healthcare data using fog-to-cloud computing

---

Thesis will be defended publicly in front of the committee composed of:

|                           |                     |               |
|---------------------------|---------------------|---------------|
| Mr. Azzeddine CHIKH       | Full Professor      | President     |
| Mrs. Nabila LABRAOUI      | Full Professor      | Supervisor    |
| Mr. Ado Adamou ABBA ARI   | Associate Professor | Co-Supervisor |
| Mr. Sofiane BOUKLI HACENE | Full Professor      | Examiner      |
| Mr. Bouabdellah KECHAR    | Full Professor      | Examiner      |
| Mr. Samir KAMECHE         | Full Professor      | Examiner      |

University Year 2022-2023



---

# Acknowledgments

Firstly, all praise and thanks go to “ALLAH” who gave me the power to beat life’s challenges and to continue my higher studies “ALHAMDULILLAH”.

At the beginning of this dissertation and the end of this journey, I would like to thank everyone who helped me to complete this work.

I would like to thank my supervisor, Mrs. Nabila LABRAOUI for her interesting comments and advice. She provided me with valuable academic suggestions, relevant research ideas, and administrative support during my research. Also, my thanks go to Mr. Ado Adamou ABBA ARI for accepting to be my co-supervisor and for his advice and tips regarding academic research.

I am pleased and want to express my thanks to the jury members who accepted the invitation and their honorary presence will, with no doubt, give this modest thesis valuable value. Thank you (1) Mr. Azzedine CHIKH, whom we were lucky to have back again as a real addition to the CS department, (2) Mr. Samir KAMECHE, one of the main pillars of our STIC Lab, (3) Mr. Bouabdellah KECHAR whose researches and contributions in the field of cybersecurity and wireless networks are indispensable and (4) Mr. Sofiane BOUKLI HACENE who agreed for being a valuable member of the jury, I am grateful to have you in my thesis committee.

I would like to express my deepest appreciation to Mr. Leandros MAGLARAS, who has supported me during my research with his guidance, and advice. His knowledge and continuous support were crucial for my research study.

I would like to express my gratitude to Mr. Joel Herve MBOUSSAM EMATI for his appreciative collaboration in my research publications and his encouragement when they were the most needed.



---

# Dedication

I proudly dedicate my dissertation work to the memory of my father. He was unable to see my graduation. This is for him.

A special feeling of gratitude to my loving mother, whose words of encouragement and push for tenacity ring in my ears.

This work is also dedicated to my lovely husband, Djelloul, who has been a constant source of support and encouragement during the challenges of studies and life. I am truly thankful for having you in my life. Without forgetting my children: Rachad, Lina and Abdurrahman, You have made me stronger, better and more fulfilled than I could have ever imagined. I love you to the moon and back. I hope the sacrifices you have endured for me to pursue this dream will be repaid to you with many opportunities for joy and success in your future.

I also dedicate this dissertation to my brother Diden and my sisters Amina and Hassiba. You were all the support that I relied and keep relying on to tackle the diverse life obstacles.

I also dedicate this dissertation to my many friends, who encouraged and supported me.

All the people in my life who touch my heart, I dedicate this research.

Hafida



---

# Abstract

Over the past few decades, the world has become more connected with the wide adoption of Internet of Things (IoT), cloud computing, and fog computing. These technologies are the driving force to collect, process, and store medical data. However, the privacy and security of health data represent major challenges. For this purpose, to enhance the security and benefit from the advantages of cloud and fog computing, a hierarchical Fog-To-Cloud (F2C) computing system was introduced which integrates the fog and the cloud in a single model.

In this thesis, we provide a comprehensive state-of-the-art that deals with the aforementioned problem in the context of IoT, F2C, and e-health. Then, we propose two contributions using several technologies. As the patient's medical data are accessible by users who have diverse privileges, we have adopted a decentralized access control system using blockchain and Self-Sovereign Identity (SSI) for privacy-preserving data. Hence, our proposed approach focuses on smart contract to conduct Role-Based Access Control policies (RBAC) and adopts the implementation of Decentralized Identifiers (DID) and Verifiable Credentials (VC) to describe advanced access control techniques for emergency cases.

Experimental results based on privacy-preserving medical records demonstrate that our proposed solution ensures a high level of security, protect data privacy, empower patients with mechanisms to preserve control over their personal information, and allow them to self-grant access rights to their medical data.

**Keywords:** Security and Privacy, E-health, IoMT, F2C, encryption, blockchain, SSI, DID, VC.





## Résumé

---

Au cours des dernières décennies, le monde est devenu plus connecté avec l'adoption généralisée de l'Internet des objets (IoT), du cloud computing et du fog computing. Ces technologies sont le moteur de la collecte, du traitement et du stockage des données médicales. Or, la confidentialité et la sécurité des données de santé représentent des enjeux majeurs. Dans ce but, pour renforcer la sécurité et bénéficier des avantages du cloud et du fog computing, un système informatique hiérarchique Fog-To-Cloud (F2C) a été introduit qui intègre le fog et le cloud dans un seul modèle.

Dans cette thèse, nous fournissons un état de l'art complet qui traite du problème susmentionné dans le contexte de l'IoT, du F2C et de la e-santé. Ensuite, nous proposons deux contributions utilisant plusieurs technologies. Comme les données médicales du patient sont accessibles par des utilisateurs qui ont des privilèges divers, nous avons adopté un système de contrôle d'accès décentralisé utilisant la blockchain et l'identité auto-souveraine (SSI) pour les données préservant la confidentialité.

Par conséquent, notre approche proposée se concentre sur le contrat intelligent pour mener des politiques de contrôle d'accès basées sur les rôles (RBAC) et adopte la mise en œuvre d'identifiants décentralisés (DID) et d'identifiants vérifiables (VC) pour décrire les techniques avancées de contrôle d'accès pour les cas d'urgence.

Les résultats expérimentaux basés sur des dossiers médicaux préservant la confidentialité démontrent que notre solution proposée assure un haut niveau de sécurité, protège la confidentialité des données, donne aux patients les moyens de conserver le contrôle de leurs informations personnelles et leur permet d'accorder eux-mêmes des droits d'accès à leurs données médicales.

**Mots-clés:** Sécurité et vie privée, e-santé, IoMT, F2C, cryptage, blockchain, SSI, DID, VC.

## ملخص

حالياً أصبح العالم أكثر ارتباطاً بظهور تقنيات إنترنت الأشياء (IoT)، الحوسبة السحابية (Cloud computing) وحوسبة الضباب (Fog computing). بفضل هذه التقنيات يتم جمع، معالجة وتخزين البيانات الطبية، إلا أن خصوصية وأمن البيانات الصحية تمثل تحديات كبيرة. فلهذا الغرض، ومن أجل تعزيز الأمن والاستفادة من مزايا الحوسبة السحابية والضبابية، تم استعمال نظام حوسبة هرمي من الضباب إلى السحابة (F2C) يدمج الضباب والسحابة في نموذج واحد.

في هذه الأطروحة، نقدم أحدث ما توصلت إليه التكنولوجيا لوضع حل للمشكلة المذكورة أعلاه في سياق إنترنت الأشياء، و F2C، والصحة الإلكترونية. بعد ذلك، نقترح مساهمتين باستخدام العديد من التقنيات.

حيث يمكن لعدة مستخدمين الوصول إلى البيانات الطبية للمريض من خلال امتيازاتهم المتنوعة، لذلك اعتمدنا نظاماً لامركزياً للتحكم في الوصول باستخدام blockchain والهوية الذاتية السيادية (SSI) من أجل الحفاظ على الخصوصية. ومن ثم، فإن نهجنا المقترح يركز على العقد الذكي لإجراء سياسات التحكم في الوصول على أساس الأدوار (RBAC) وعلى التعريفات اللامركزية (DID) وبيانات الاعتماد القابلة للتحقق (VC) لاقتراح تقنية متقدمة للتحكم في الوصول إلى البيانات الطبية للمريض في حالات الطوارئ. تظهر النتائج التجريبية للحفاظ على الخصوصية أن حلنا المقترح يضمن مستوى عالٍ من الأمن، وحماية خصوصية البيانات، ويقدم للمرضى آليات للحفاظ على معلوماتهم الشخصية، والسماح لهم بمنح حقوق الوصول إلى بياناتهم الطبية.

**الكلمات المفتاحية:** إنترنت الأشياء، الحوسبة السحابية وحوسبة الضباب، خصوصية وأمن البيانات، الصحة الإلكترونية، التعريفات اللامركزية، بلوكتشاين والهوية الذاتية السيادية.



---

# List of publications

## International Journals

- Hafida Saidi, Nabila Labraoui, Ado Adamou Abba Ari, Leandros Maglaras, and Joel Herve Mboussam Emati. "DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data." IEEE Access (2022). DOI: 10.1109/ACCESS.2022.3207803  
URL:<https://ieeexplore.ieee.org/abstract/document/9895264>
- Hafida Saidi, Nabila Labraoui, Ado Adamou ABBA ARI. "A secure health monitoring system based on Fog to Cloud computing", 2022, Int. J. of Medical Engineering and Informatics, Inderscience. DOI: 10.1504/IJMEI.2022.10050253  
URL: <http://dx.doi.org/10.1504/IJMEI.2022.10050253>

## International Conferences

- Hafida Saidi, Nabila Labraoui, Ado Adamou Abba Ari, and Djelloul Bouida. "Remote health monitoring system of elderly based on Fog to Cloud (F2C) computing." In 2020 international conference on intelligent systems and computer vision (ISCV), pp. 1-7. IEEE, 2020. DOI: 10.1109/ISCV49265.2020.9204096  
URL:<https://ieeexplore.ieee.org/abstract/document/9204096>

- Hafida Saidi, Nabila Labraoui, Ado Adamou Abba Ari, Ikram Semahi, and Bouchra Ramdane Mamcha. "Real-time Aging Friendly fall detection system." In 2019 6th International Conference on Image and Signal Processing and their Applications (ISPA), pp. 1-6. IEEE, 2019. DOI: 10.1109/ISPA48434.2019.8966857 URL:<https://ieeexplore.ieee.org/abstract/document/8966857>




---

# Contents

|   |          |
|---|----------|
| Acknowledgments   | i        |
| Dedication  | ii       |
| Abstract  | iii      |
| Résumé  | iv       |
| Contents  | xi       |
| List of Figures   | xiii     |
| List of Tables  | xiv      |
| List of Acronyms  | xv       |
| General Introduction                                      | 1        |
| <b>I LITTERATURE REVIEW</b>                               | <b>5</b> |
| <b>1 E-health in the sphere of IoMT and F2C computing</b> | <b>6</b> |
| 1.1 Introduction . . . . .                                | 7        |
| 1.2 Background knowledge . . . . .                        | 7        |
| 1.2.1 E-health system . . . . .                           | 8        |
| 1.2.2 Internet of Medical Things (IoMT) . . . . .         | 10       |
| 1.2.3 Computing models . . . . .                          | 11       |
| 1.3 Impact of IoMT in an e-health system . . . . .        | 16       |

---

|          |   |           |
|----------|---|-----------|
| 1.3.1    | Influence of IoMT on an healthcare systems . . . . .                  | 16        |
| 1.3.2    | IoMT applications in e-health systems . . . . .                       | 19        |
| 1.4      | E-health applications using F2C computing . . . . .                   | 21        |
| 1.4.1    | F2C-based e-health architectures . . . . .                            | 21        |
| 1.4.2    | Benefits of F2C for e-health systems . . . . .                        | 22        |
| 1.4.3    | F2C data management-based e-health systems . . . . .                  | 23        |
| 1.5      | F2C-IoMT System . . . . .   | 25        |
| 1.6      | Summary . . . . .   | 25        |
| <b>2</b> | <b>Security and Privacy issues in E-health systems</b>                | <b>27</b> |
| 2.1      | Introduction . . . . .  | 28        |
| 2.2      | Security and privacy goals and concerns in e-health systems . . . . . | 28        |
| 2.3      | Security issues in e-health based F2C-IoMT systems . . . . .          | 29        |
| 2.3.1    | Basic security consideration in the F2C system . . . . .              | 30        |
| 2.3.2    | Security requirements in IoMT Systems . . . . .                       | 30        |
| 2.3.3    | Security challenges and directions in the F2C-IoMT system . . . . .   | 32        |
| 2.3.4    | Most potential attacks in the F2C-IoMT system . . . . .               | 34        |
| 2.4      | Privacy issues in e-health based F2C-IoMT systems . . . . .           | 35        |
| 2.4.1    | Privacy: A crucial parameter . . . . .                                | 36        |
| 2.4.2    | Privacy Requirements in e-health systems . . . . .                    | 41        |
| 2.5      | Related works . . . . .   | 42        |
| 2.5.1    | Centralized-based approaches . . . . .                                | 42        |
| 2.5.2    | Distributed-based approaches . . . . .                                | 43        |
| 2.5.3    | Trusted Third-Party approaches . . . . .                              | 45        |
| 2.6      | Summary . . . . .   | 46        |
| <b>3</b> | <b>Data security and privacy techniques</b>                           | <b>48</b> |
| 3.1      | Introduction . . . . .  | 49        |
| 3.2      | Security and privacy-preserving techniques . . . . .                  | 49        |
| 3.2.1    | Restriction-based mechanisms . . . . .                                | 49        |
| 3.2.2    | Perturbation-based mechanisms . . . . .                               | 54        |
| 3.2.3    | Aggregation-based mechanisms . . . . .                                | 56        |
| 3.2.4    | Decentralized-based mechanisms . . . . .                              | 59        |
| 3.3      | Related works . . . . .   | 66        |
| 3.3.1    | Encryption techniques . . . . .                                       | 66        |
| 3.3.2    | Access control techniques . . . . .                                   | 67        |

---

|           |   |           |
|-----------|---|-----------|
| 3.3.3     | Differential Privacy . . . . .  | 68        |
| 3.3.4     | Anonymization/Pseudonymization techniques . . . . .   | 68        |
| 3.3.5     | Homomorphic encryption techniques . . . . .   | 69        |
| 3.3.6     | Blockchain techniques . . . . .   | 69        |
| 3.3.7     | Self-Sovereign Identity Technology . . . . .  | 70        |
| 3.4       | Summary . . . . .   | 71        |
| <br>      |   |           |
| <b>II</b> | <b>CONTRIBUTIONS</b>  | <b>72</b> |
| <br>      |   |           |
| <b>4</b>  | <b>A secure health monitoring system based on Fog to Cloud computing</b>                        | <b>73</b> |
| 4.1       | Introduction . . . . .  | 74        |
| 4.1.1     | Motivation . . . . .  | 74        |
| 4.2       | F2C architecture . . . . .  | 75        |
| 4.3       | System model and design goals . . . . .   | 76        |
| 4.3.1     | System model . . . . .  | 76        |
| 4.3.2     | Design Goals . . . . .  | 78        |
| 4.4       | Security Model . . . . .  | 79        |
| 4.4.1     | Lightweight Security Scheme (L2S) . . . . .   | 79        |
| 4.4.2     | Case study: fall detection algorithm . . . . .  | 85        |
| 4.5       | Security Analysis . . . . .   | 86        |
| 4.5.1     | Security and Confidentiality . . . . .  | 86        |
| 4.5.2     | Privacy . . . . .   | 86        |
| 4.6       | Performance evaluation . . . . .  | 86        |
| 4.6.1     | Simulation setup . . . . .  | 87        |
| 4.6.2     | Results and discussion . . . . .  | 88        |
| 4.7       | Summary . . . . .   | 91        |
| <br>      |   |           |
| <b>5</b>  | <b>A novel decentralized framework for privacy-preserving and securing medical data sharing</b> | <b>93</b> |
| 5.1       | Introduction . . . . .  | 94        |
| 5.1.1     | Motivation . . . . .  | 95        |
| 5.2       | Background knowledge . . . . .  | 96        |
| 5.2.1     | Self-Sovereign Identity (SSI) . . . . .   | 96        |
| 5.2.2     | Blockchain . . . . .  | 102       |
| 5.2.3     | Access control . . . . .  | 105       |
| 5.2.4     | Zero-Knowledge Proof (ZKP) . . . . .  | 109       |

|       |   |            |
|-------|---|------------|
| 5.3   | Models and security requirements . . . . .  | 109        |
| 5.3.1 | System model . . . . .  | 110        |
| 5.3.2 | Adversary model . . . . .   | 112        |
| 5.3.3 | Security requirements and design goal . . . . .                                   | 114        |
| 5.4   | Proposed DSMAC scheme . . . . .   | 115        |
| 5.4.1 | Towards a decentralized access control scheme . . . . .                           | 115        |
| 5.4.2 | Decentralized Access Control Scheme Based-SSI model . . . . .                     | 118        |
| 5.4.3 | Decentralized Access Control scheme using Blockchain-based SSI<br>model . . . . . | 121        |
| 5.5   | Experiments and Results . . . . .   | 126        |
| 5.5.1 | Experimental setup . . . . .  | 126        |
| 5.5.2 | Experimental Analysis . . . . .   | 132        |
| 5.6   | Security and privacy analysis . . . . .   | 137        |
| 5.6.1 | Comparison of security properties . . . . .                                       | 137        |
| 5.6.2 | Privacy protection . . . . .  | 139        |
| 5.6.3 | Access Control protection . . . . .   | 139        |
| 5.6.4 | Attacks analysis . . . . .  | 140        |
| 5.7   | Summary . . . . .   | 142        |
|       | <b>General Conclusion</b>   | <b>143</b> |
|       | <b>Publications</b>   | <b>145</b> |
|       | <b>Bibliography</b>   | <b>150</b> |




---

# List of Figures

|             |   |    |
|-------------|---|----|
| Figure 1.1: | IoT applications enabled by cloud . . . . .                           | 12 |
| Figure 1.2: | Comparison between Cloud computing (a) and Fog computing (b). . . . . | 15 |
| Figure 1.3: | Medical wearable devices. . . . .                                     | 18 |
| Figure 1.4: | Benefits of IoMT . . . . .  | 19 |
| Figure 1.5: | F2C-based e-health system . . . . .                                   | 22 |
| Figure 2.1: | Security and privacy goals in healthcare systems . . . . .            | 28 |
| Figure 2.2: | F2C layer security . . . . .  | 30 |
| Figure 2.3: | Basic security requirements related to e-health systems . . . . .     | 33 |
| Figure 2.4: | Most potential attacks in F2C systems . . . . .                       | 35 |
| Figure 3.1: | Data encryption techniques . . . . .                                  | 51 |
| Figure 3.2: | Role-based access control (RBAC) . . . . .                            | 54 |
| Figure 3.3: | Differential privacy technique . . . . .                              | 55 |
| Figure 3.4: | Self-sovereign Identity Ecosystem . . . . .                           | 64 |
| Figure 4.1: | System overview . . . . .   | 77 |
| Figure 4.2: | Flow chart of L2S . . . . .   | 84 |
| Figure 4.3: | Main page of FogWorkflowSim . . . . .                                 | 88 |
| Figure 4.4: | Summary of experimental results . . . . .                             | 89 |
| Figure 4.5: | Latency comparison . . . . .  | 90 |
| Figure 4.6: | Energy consumption comparison . . . . .                               | 90 |
| Figure 4.7: | Execution cost comparison . . . . .                                   | 91 |
| Figure 5.1: | The basic components of DID architecture . . . . .                    | 99 |

---

|              |   |     |
|--------------|---|-----|
| Figure 5.2:  | DID Format . . . . .  | 99  |
| Figure 5.3:  | Example of a Verifiable Credential . . . . .                    | 100 |
| Figure 5.4:  | Verifiable Credential Lifecycle . . . . .                       | 101 |
| Figure 5.5:  | Simplified blockchain . . . . .                                 | 103 |
| Figure 5.6:  | Merkle tree . . . . .   | 104 |
| Figure 5.7:  | Basic elements of RBAC . . . . .                                | 106 |
| Figure 5.8:  | The ABAC Architecture . . . . .                                 | 108 |
| Figure 5.9:  | System overview . . . . .                                       | 110 |
| Figure 5.10: | Sequence diagram of DID generation and VC issuance operations   | 120 |
| Figure 5.11: | The structure and resolution of DID Document (DDO) . . . . .    | 120 |
| Figure 5.12: | Sequence diagram of RDAC-PDC approach . . . . .                 | 122 |
| Figure 5.13: | VON network . . . . .   | 128 |
| Figure 5.14: | Running of ACA-Py agent (Patient) . . . . .                     | 129 |
| Figure 5.15: | Docker list containers . . . . .                                | 129 |
| Figure 5.16: | Postman API . . . . .   | 130 |
| Figure 5.17: | Ledger transactions . . . . .                                   | 131 |
| Figure 5.18: | Transaction time comparison of RDAC and ADAC models . . . . .   | 133 |
| Figure 5.19: | Transaction throughput of RDAC and ADAC models. . . . .         | 135 |
| Figure 5.20: | Transaction latency of RDAC and ADAC models . . . . .           | 135 |
| Figure 5.21: | Time while performing data encryption . . . . .                 | 136 |
| Figure 5.22: | CPU and memory usage while performing data encryption . . . . . | 137 |



---

## List of Tables

|  |     |
|--|-----|
| Table 2.1: Security and privacy characteristics open challenges . . . . .      | 29  |
| Table 2.2: Security and privacy requirements as recommended by HIPAA .         | 31  |
| Table 2.3: Privacy design strategies . . . . .                                 | 39  |
| Table 2.4: List of some privacy approaches. . . . .                            | 46  |
| Table 4.1: Comparison of performance parameters of two different environments. | 89  |
| Table 5.1: Tools used in the experimentation . . . . .                         | 126 |
| Table 5.2: Encryption time . . . . .   | 136 |
| Table 5.3: Comparison between related works and our DSMAC model . . .          | 138 |



---

# List of Acronyms

**AAI:** Ambient Assisted Living  
**ABAC:** Attribute-Based Access Control  
**ABE:** Attribute-Based Encryption  
**ACA-Py:** Aries Cloud Agent Python  
**ACL:** Access Control List  
**ADAC:** Attributes-based Decentralized Access Control  
**AES:** Advanced Encryption Standard  
**AMN:** Authorization Management Node  
**AN:** Authenticator Node  
**ANSI:** American National Standards Institute  
**AP:** Adaptive Permissions  
**AR:** Access Requester  
**ARRA:** American Recovery and Reinvestment Act  
**CC:** Contextual Constraints  
**CD:** Contextual conditions  
**CP-ABE:** Ciphertext-Policy Attribute-Based Encryption  
**DAC:** Discretionary Access Control  
**DDO:** DID Document  
**DDoS:** Distributed Denial of Service  
**DES:** Data Encryption Standard  
**DID:** Decentralized IDs  
**DO:** Data Owner  
**DoS:** Denial DoSf Service  
**DP:** Default Permissions  
**DSMAC:** Decentralized Self-Management of data Access Control  
**ECC:** Elliptic-Curve Cryptography  
**ECG:** ElectroCardioGram  
**EEFC:** Efficient Energy Fog-based Computing  
**E-health:** Electronic-health  
**EHR:** Electronic Health Records  
**EMR:** Electronic Medical Records  
**EMT:** Emergency Medical Technicians  
**F2C:** Fog to Cloud

**FHE:** Fully Homomorphic Encryption  
**HE:** Homomorphic Encryption  
**HIPAA:** Health Insurance Portability and Accountability Act  
**ICT:** Information and Communication Technologies  
**IoT:** Internet of Things  
**IoMT:** Internet of Medical Things  
**L2S:** Lightweight Security Scheme  
**MAC:** Mandatory Access Control  
**MPC:** Multi-Party Computation  
**NFC:** Near-Field Communication  
**NIST:** National Institute of Standards and Technology  
**NIZKP:** Non-Interactive Zero-Knowledge Proofs  
**NHS:** National Health Service  
**OrBAC:** Organization-Based Access Control  
**P2P:** Peer-To-Peer  
**PA:** Permissions Assignment  
**PAP:** Policy Administration Point  
**PDC:** Policy Decision smart Contract  
**PDP:** Policy Decision Point  
**PEP:** Policy Enforcement Point  
**PHE:** Partially Homomorphic Encryption  
**PHI:** Personal Health Information  
**PIP:** Policy Information Point  
**PKI:** Public Key Infrastructure  
**PoA:** Proof of Authority  
**PoS:** Proof of Stake  
**PoW:** Proof of Work  
**PRP:** Policy Retrieval Point  
**RBAC:** Role-Based Access Control  
**REM:** Remote Health Monitoring  
**RFID:** Radio Frequency Identification  
**RSA:** Rivest–Shamir–Adleman  
**RDAC:** Role-Based Decentralized Access Control  
**SC:** Smart Contract  
**SSI:** Self-Sovereign Identity  
**SSL/TLS:** Secure Sockets Layer /Transport Layer Security  
**TA:** Trusted Authority  
**UA:** Users Assignment  
**UTXO:** Unspent Transaction Output  
**VC:** Verifiable Credentials  
**W3C:** World Wide Web Consortium  
**XACML:** Extensible Access Control Markup Language  
**ZKP:** Zero Knowledge Proofs



---

# General Introduction

To enhance the quality of patients' life, technological mechanisms, and advanced solutions have been proposed by research communities to manage medical records and solve health-related issues. Indeed, the creation of the Electronic-health (E-health) system (Monteiro et al., 2021) solved many challenges reliable to traditional healthcare systems. E-health systems are based on Information and Communication Technologies (ICT) which improve patient conditions, decrease costs, enhance patient quality of life, and increase collaboration and efficiency of health services. Additionally, e-health systems are accomplished through several techniques including ubiquitous data access, remote patient monitoring, immediate clinical interventions, decentralized e-health records, etc.

On the other hand, the integration of Internet of Things (IoT) (Djam-douou et al., 2023), cloud computing, and fog computing can provide a powerful solution for the healthcare environment by combining the strengths of each technology. IoT devices can collect and transmit medical data, cloud computing can provide large-scale data storage and processing capabilities, and fog computing can provide edge computing capabilities for real-time data processing and decision-making. Together, these technologies can enable new applications such as real-time monitoring.

However, these technologies can present several challenges, and their combination is a complex task that requires a holistic approach to address these issues.

## **Problem statement**

With the increasing use of e-health systems, there are several security and privacy challenges that must be addressed. E-health systems manage sensitive personal and medical information. The leakage of this information causes financial losses and also breaches the most fundamental right of a patient, i.e. right to privacy. Privacy must be protected and respected, even if data is shared for research or treatment purposes (Edwards et al., 2016). Hence, e-health systems must comply with regulations such as HIPAA (Health Insurance Portability and Accountability Act) (HiPAA, 2010), which sets standards for protecting sensitive patient data.

Overall, the e-health field requires a multi-faceted approach to security and privacy that includes strong technical controls, policies, and procedures, as well as regular monitoring, testing, and incident response planning.

## **Thesis motivation and objectives**

Medical data is a valuable resource for research and innovation, but it is necessary to protect patient privacy when sharing data. Thus, preserving the security and privacy of medical data is critical for protecting patients' rights, maintaining trust in the healthcare system, and enabling research and innovation while complying with legal and regulatory requirements. However, inadequate security and privacy measures can put patients at risk by exposing personal information, or by allowing unauthorized access to medical devices or systems. In fact, traditional privacy preservation mechanisms are no longer sufficient due to the volume, variety, and velocity of the collected big data. They have several limitations and impacts on the data utility, accuracy, and system efficiency. For this purpose, there is a need to design efficient solutions for privacy-preserving data sharing to minimize the impact of breaching attacks and encourage the development and improvement of big-data services.

The different objectives of this thesis can be classified into two sections, the theoretical objectives, and the technical objectives.

- The theoretical objectives are as follows:
  1. Security and privacy requirements and challenges are analyzed.
  2. Security attacks in the F2C-IoMT system are described.
  3. Some existing security solutions are reviewed.
  
- The technical objectives are:
  1. A novel security framework is designed to be adopted into the F2C system.
  2. A decentralized access control model based on blockchain and SSI system is implemented to protect patients' medical data.
  3. Smart contract functionalities are deployed to issue or modify the Role-Based Access Control (RBAC) policies.
  4. An Attribute-based Access Control (ABAC) mechanism is implemented based on the Decentralized Identifier (DID) document.

## Thesis Outline & Contributions

This thesis deals with security and privacy problems and is composed of two main parts:

### 1. LITERATURE REVIEW:

It is done in three chapters, in which we give an introduction to the stated problem accompanied by related works. It is outlined as follows:

- **Chapter 1:** starts by giving basic notions on e-health systems, Internet of Medical Things (IoMT), and Fog to Cloud computing (F2C). Then, it presents the impact of IoMT and F2C on e-health systems.
- **Chapter 2:** describes security and privacy issues in general. It presents the most basic and potential security considerations for the F2C system and analyses the most potential attacks in IoMT-based F2C computing in e-health systems.



- **Chapter 3:** presents introductions to security and privacy techniques which will be helpful to understand the remainder of this thesis. Also, a review of the works related is discussed.

## 2. SCIENTIFIC CONTRIBUTIONS:

We start proposing solutions and giving contributions to our research field, this is done in two chapters outlined as follows:

- **Chapter 4:** gives the first contribution in kind of a secure health monitoring system based on fog to cloud computing. The chapter provides a model which demonstrates and describes the benefits of using F2C computing in the e-health domain. Then a security model is presented to ensure the security and privacy required by HIPAA regulations. In this context, a Lightweight Security Scheme (L2S) is proposed.
- **Chapter 5:** proposes a novel Decentralized Self-Management of data Access Control (DSMAC) system using a blockchain-based Self-Sovereign Identity (SSI) model for privacy-preserving medical data. DSMAC implements Decentralized Identifiers (DID) and Verifiable Credentials (VC) to specify advanced access control policies for emergencies. It also uses smart contracts to construct role-based access control policies. The performance evaluation step demonstrates that DSMAC can satisfy the privacy, scalability, and sustainability requirements, and manage emergency cases.

In the final stage, we give a general conclusion to the thesis as a whole, and future work that this thesis had given as insights.

---

## **Part I**

# **LITTERATURE REVIEW**

Chapter

**1**


---

# E-health in the sphere of IoMT and F2C computing

---

## Contents

|            |  |           |
|------------|--|-----------|
| <b>1.1</b> | <b>Introduction</b>                              | <b>7</b>  |
| <b>1.2</b> | <b>Background knowledge</b>                      | <b>7</b>  |
| 1.2.1      | E-health system                                  | 8         |
| 1.2.2      | Internet of Medical Things (IoMT)                | 10        |
| 1.2.3      | Computing models                                 | 11        |
| <b>1.3</b> | <b>Impact of IoMT in an e-health system</b>      | <b>16</b> |
| 1.3.1      | Influence of IoMT on an healthcare systems       | 16        |
| 1.3.2      | IoMT applications in e-health systems            | 19        |
| <b>1.4</b> | <b>E-health applications using F2C computing</b> | <b>21</b> |
| 1.4.1      | F2C-based e-health architectures                 | 21        |
| 1.4.2      | Benefits of F2C for e-health systems             | 22        |
| 1.4.3      | F2C data management-based e-health systems       | 23        |
| <b>1.5</b> | <b>F2C-IoMT System</b>                           | <b>25</b> |
| <b>1.6</b> | <b>Summary</b>                                   | <b>25</b> |

---

## 1.1 Introduction

This preliminary chapter aims to give a start-up setup to the LITERATURE REVIEW part and the thesis as a whole. Starting with basic notions, we provide an introduction to the e-health system, IoMT, and Fog to Cloud (F2C) technologies. Additionally, we highlight the implications of the IoMT and F2C technologies in e-health systems. Next, The chapter details the different e-health applications. Finally, we give a summary of the current chapter.

Nowadays, different technologies like smartphones, wearable devices, and Internet of Things (IoT) devices, can collect information about human health to provide effective healthcare. Thus, the Internet of Medical Things (IoMT) is one of the main alternatives to following up the patients and developing healthcare systems. They can collect different vital signals, such as heart rate, body temperature, blood pressure, etc. Then the vital data can be sent to a medical center. If an emergency occurs, the system can generate an alarm.

## 1.2 Background knowledge

In this section, the key technologies that support the proposal of our research are briefly introduced, more specifically, these are e-health systems, IoT, and fog to cloud computing. Integrating medical systems with IoT features gives rise to the Internet of Medical Things (IoMT) which proves the quality of medical services, and enhances the associated human users' satisfaction. Therefore, IoMT is rapidly evolving, offering promising technological, financial, and social prospects in multiple areas, such as industrial, smart cities, agriculture, and health systems (Monteiro et al., 2021). Moreover, the Internet of Medical Things (IoMT) technology has been commonly applied due to its high performance, saving time, and efforts of patients/specialists. Besides, it enhances patient care, such as monitoring their

medications and the diagnosis of different illnesses, tracking their hospital admission location, and obtaining and analyzing data.

### **1.2.1 E-health system**

Wireless and mobile technologies play an important role in the birth of new paradigms of healthcare and services. The term "digital health," also known as "e-health," emerged to define the ICTs' application in the healthcare area, providing IoT resources to deliver optimal diagnosis and improve patient care. E-health system includes innovations in a variety of fields, such as hospital management, doctor-patient interaction, and research (Saha et al., 2019).

#### **1.2.1.1 Overview**

We can define e-health as the fact of providing health professionals with tools to improve the quality and efficiency of care while reducing costs, allowing them to collect, process, store, restore and exchange health data. In addition, the e-health system offers enormous opportunities to patients by helping them to improve their quality of life with continuous monitoring of their daily activities and providing the needed healthcare consultation and alarming the hospitals in case of critical situations. The particularity of e-health is that it is not reserved exclusively for health professionals, unlike telemedicine for example, but also desired by patients or consumers (Saha et al., 2019).

#### **1.2.1.2 Benefits of e-health system**

The use of new techniques, tools, and channels in the e-health environment results in several advantages (Saha et al., 2019):

- Enhanced patient monitoring can make it easy for medical professionals to select the best treatments or detect illnesses early on.

- Improved access to healthcare and innovation enhances access to healthcare for more people, particularly those at risk of exclusion, i.e more equal opportunities for all.
- When people are more informed and empowered to take control of their health, better health decisions can be taken.
- Promoting healthier behaviors including tracking our food intake, exercise levels, sleep duration and quality, and heart rate.
- More smart hospitals to minimize human error.

### 1.2.1.3 Technologies used in the e-health system

To digitize the health sector, new technologies are used, including (Saha et al., 2019):

- *Internet of Things (IoT)*: The IoT aids to personalize healthcare, minimizing the risk of accidents, and reduce waiting times, and saving costs.
- *Big data*: When analyzing medical big data, it is possible to create customized treatments and identify risk factors and probable drug adverse effects.
- *Artificial Intelligence*: AI can assist healthcare professionals in making better decisions and providing better care. AI was also employed during the coronavirus crisis to determine the antibody sequence and its suitability for potential treatments.
- *Blockchain*: Blockchain enables secure access to a patient's medical records, improving data management.
- *Chatbots*: These programs give patients and doctors a way to communicate more quickly and directly. During the COVID-19 epidemic, the World Health Organization established one of these channels.

## **1.2.2 Internet of Medical Things (IoMT)**

Integration of e-health systems with IoT technology gives rise to the Internet of Medical Things (IoMT) technology. Several aims of the IoMT technology exist, including the collection and exchange of medical data among IoT devices and the monitoring of patients through the integration of computing devices (Madiyal, 2022).

### **1.2.2.1 Overview**

IoMT is a network of health applications, medical devices, and other appliances that are interconnected through wireless connectivity. It represents an extension of IoT in the healthcare industry for remote monitoring of patients through medical sensors. This optimizes how the patient information is monitored in real-time and improves data accuracy. It also reduces healthcare costs for organizations and increases their efficiency in carrying out operations (Madiyal, 2022).

### **1.2.2.2 IoT vs. IoMT**

Both IoT and IoMT are built on the same concept of interconnected devices that can send and receive data over a wireless network. IoMT can be regarded as an extension of the IoT technology that is specialized for the healthcare sector (Madiyal, 2022).

### **1.2.2.3 Example of IoMT devices**

IoMT devices can be categorized into the following types (Madiyal, 2022):

- *Fitness wearable devices*

They include products that store, transmit, and analyze the physical activity of users like smartwatches.

- *Remote patient monitoring devices*

The IoMT devices enable hospital professionals to virtually visit their patients and keep a check on them remotely.

- *Smart pills*

Smart pills are digestible sensors that track how the patient reacts to the consumed medication. These sensors get activated upon reaching the stomach following which the data is sent to the wearable patch attached to the patient's arm.

- *Clinical grade wearables*

These clinical-grade IoMT devices come with health-tracking sensors that allow doctors to monitor the real-time health status of their patients.

- *Point Of Care Device*

These IoMT devices make healthcare more accessible to patients through self-serving diagnostics solutions thus preventing the need to visit hospitals.

### 1.2.3 Computing models

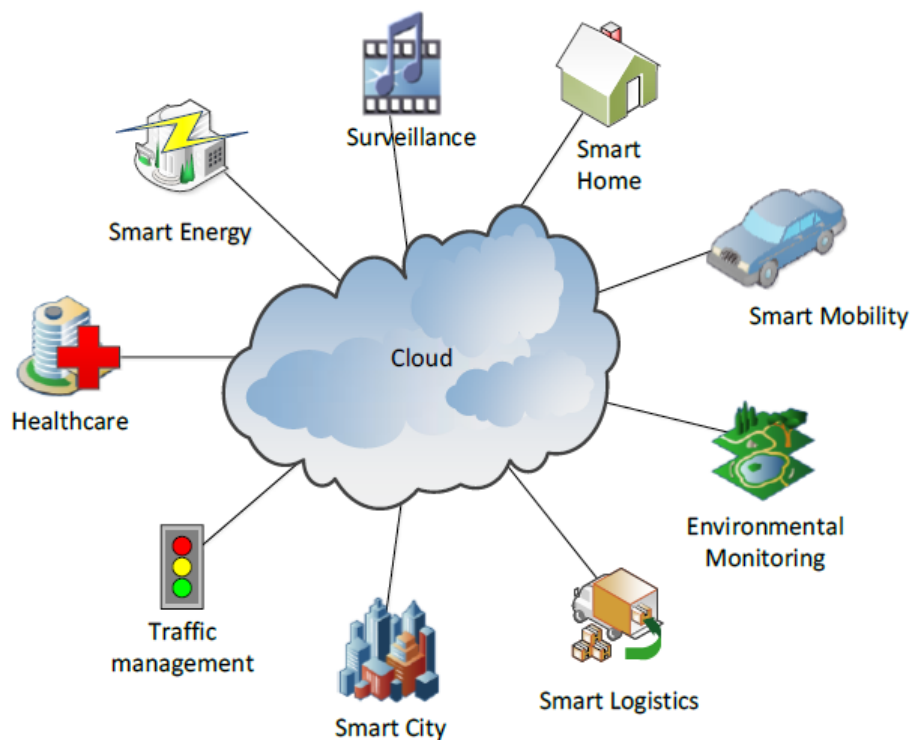
At any time, various data of different patients and IoT devices are sensed and collected. However, due to the limited computation and storage capacities, smart hospitals can deploy computing models to store this vast amount of data such as cloud computing and fog computing (Sahu et al., 2021).

#### 1.2.3.1 Cloud computing

In recent years, cloud-based health applications was developed rapidly (Mehmood et al., 2018). It is the top layer of the architecture which contains a highly distributed computing data center and storage capacity that stores medical data and implements data analytics of health data. Cloud computing provides centralized controlling and powerful computing capacities (Ari et al., 2020), it increases reliability and flexibility



and reduces administrators' tasks (Ari et al., 2020). The adoption of cloud computing has motivated several IoT services such as healthcare, smart mobility systems, smart home, environment monitoring, etc., as shown in Figure 1.1. Based on body sensors, healthcare services may be able to provide remote supervision to patients at their homes (Sun et al., 2019). Moreover, to provide flexible resources, faster innovation, reliability, and massive computing power, cloud computing can provide everything as a service like a platform as a service, infrastructure as a service, and software as a service (Sun et al., 2019).



**Figure 1.1.** *IoT applications enabled by cloud*

Furthermore, cloud computing can be divided into different sub-layers (Sun et al., 2019):

- *Data management sub-layer:* This sub-layer includes the data from multiple sources and stores them safely and securely, such as EHR. Consequently, data can be accessed anytime, anywhere, and when required by users.
- *Connectivity sub-layer:* This sub-layer has a variety of mechanisms to establish connectivity between sensors and cloud computing.

- *Application sub-layer*: Different services provided by the application sub-layer such as:
  - *Big data analytics*: which analyzes the aggregated health data.
  - *Rule engine*: This creates appropriate events, alarms, and notifications after analyzing the medical data.
  - *Dashboard*: This allows the users to visualize, configure, control, and share their data.

Despite the great advantages of the cloud, its major limitations are the high service response time (Xu et al., 2020), connecting various types of devices directly to the cloud, and privacy and security issues. So, to address these challenges, fog computing and edge computing are used (Mukherjee et al., 2018).

### 1.2.3.2 Fog computing

Fog computing is an extension of cloud computing (Farahani et al., 2018), its primary goal is decreasing the security gaps and providing computing resources closer to end-user devices (Bakhtyan and Zahary, 2018). It provides real-time data processing, networking, storage, and computing power (Mukherjee et al., 2018).

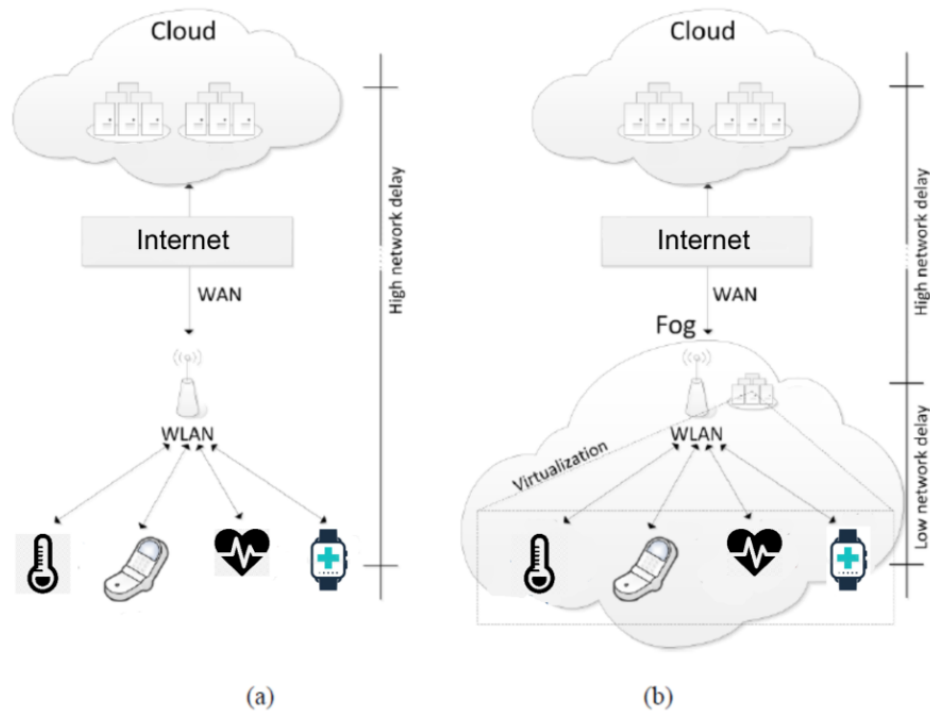
However, it is not as powerful as cloud computing. For those reasons, several research exists in this field Dolui and Datta (2017), considered fog computing as a particular implementation of edge computing. Also, Sood and Mahajan (2018) presented a real-time system based on both IoT healthcare and fog computing, it aims to detect a hypertension attack of the patient. However, these applications cause a major issue in terms of preserving the patient's privacy and security of health data. Similarly, to save and optimize energy consumption, Isa et al. (2018) presented a healthcare IoT applications-based fog computing, called EEFC (Efficient Energy Fog-based Computing) model. Furthermore, the main advantages that may be obtained from fog computing and the proximity between end devices are (Farahani et al., 2018):

1. Enhance and preserve data security and privacy since personal data can be processed at fog resources.
2. Minimize bandwidth and energy consumption.
3. Minimize connection costs for end-users.

Moreover, the different stages of data processing at the fog layer are, as follows (Masip-Bruin et al., 2016b):

- *Data aggregation and filtering:* Usually data contains noises and outliers which arrive from the sensors. Therefore, the fog layer filters and removes all invalid and unnecessary data using the aggregation process. Aggregation is done on data received from medical devices before uploading to the cloud.
- *Local storage:* The fog layer is responsible for storing temporary data in the temporary local repository. Data is stored in an encrypted or compressed format based on its importance. The data can be deleted from the temporary storage once it has been sent to the cloud.
- *Data compression:* To decrease communication latency and energy consumed during a transaction, data compression is applied. Hence, data compression is more suitable in the case of resource-constrained sensors, due to limitations such as battery lifetime and available processing power.
- *Data analysis:* By implementing data analysis in the fog layer, it improves the ability to detect emergencies and react more quickly. Therefore, local data analysis enhances the system's reliability and consistency.

Figure 1.2 compares cloud and fog architectures, in terms of latency. We can notice that the fog provides a low latency by using other resources. Nevertheless, an effective and coordinated management of the variety of resources deployed at fog and cloud computing is required. Thus, the next section introduces a novel computing paradigm designed to fulfill these requirements (Sood and Mahajan, 2018).



**Figure 1.2.** Comparison between Cloud computing (a) and Fog computing (b).

### 1.2.3.3 Fog to Cloud computing (F2C)

Fog to Cloud computing (F2C) is a novel computing paradigm and innovative model that has been recently proposed (Masip-Bruin et al., 2016b). It is conceived as a collection of hierarchically distributed layers, combining all available resources from the edge to the cloud, where varied resources are hierarchically and dynamically allocated. The F2C model can also be collaborative, because resources needed to run a service may be based either in the fog, the cloud, or both. Thus, F2C contributes to enhancing the synergy between cloud and fog computing (Masip-Bruin et al., 2016a). The different tasks performed by F2C computing are: (i) the fog receives data from IoT devices in real-time, (ii) then it runs applications for real-time control and analytics. (iii) Finally, it provides transient storage and sends periodic data to the cloud.

Hence, the primary benefits of performing data sharing via an F2C computing model are (Masip-Bruin et al., 2016b):

1. Decrease the requirement for high performance and bandwidth in cloud computing.

2. Provide computing resources, such as real-time processing with strict latency requirements, closer to end-user devices.
3. Enhance the privacy protection functions.

However, implementation of such architecture introduces several issues such as cloud and fog identification, semantic adaption, resource discovery and service allocation, as well as coordinated layer orchestration. Some of these challenges are being addressed by an H2020 European project called mF2C (Salis, 2022), which aims to design and implement the F2C architecture in a real environment, for the first time.

### **1.3 Impact of IoMT in an e-health system**

IoT has been adopted by several sectors of society, such as smart agriculture, smart transportation, smart cities, smart energy, and smart healthcare (Sood and Mahajan, 2018). The healthcare sector is one of the first to adopt IoT technologies. In this regard, the term IoMT (Kotronis et al., 2019) has emerged to deliver high-quality healthcare services, such as the collection of a patient's medical data using smart wearable devices based on IoT technology (Sahu et al., 2021). Therefore, IoMT are crucial in the development of an efficient medical system that can facilitate a better life for the patients, reduce the medical load of the health centers and doctors, and improve real-time monitoring.

#### **1.3.1 Influence of IoMT on an healthcare systems**

IoMT has transformed the healthcare industry and influenced the life of patients by improving their quality of life and providing a variety of healthcare applications based on sensing technologies, communication protocols, and data analytics techniques. In recent years, a lot of healthcare applications have introduced IoMT technology such as the automatic monitoring of patients via the use of bio-medical devices, Radio Frequency Identification (RFID) sensing technologies for personal healthcare,

platforms for fast routing of ambulances within the context of smart ambulance systems (Sahu et al., 2021), etc.

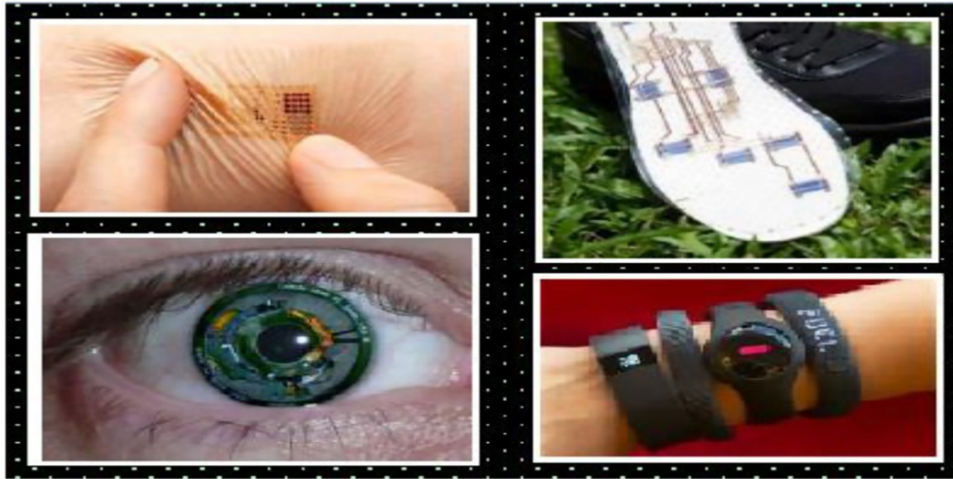
Moreover, high availability and performance are essential in the e-health systems, since any information delay may be crucial for the patient's life. However, IoMT alone can not support the complexity of e-health applications because sensors can generate a big volume of data, and the IoMT devices do not have enough resources to process and store this data. Thus, cloud and fog technologies emerge to mitigate the IoMT limitations. Some of the IoMT technologies used in the e-health system are discussed in the following subsection.

### **1.3.1.1 Wearable devices and Sensors**

As shown in Figure 1.3, sensors and wearable devices collect physiological information from the human body and they are used for real-time monitoring activities such as cardiac health monitoring (Tsai et al., 2020), fall detection (Saidi et al., 2019), sleep pattern monitoring, and so on. Thus, they should be able to notify patients and healthcare professionals when a critical situation occurs. Seneviratne et al. (2017) have talked about various wrist-worn devices, including Apple iWatch, Samsung Gear S2, Fitbit Flex, Empatica, and Pebble Time. Also, different wearable devices and sensors have been explored by several such as smartwatches, headbands, camera clips, and various embedded sensors in clothes. These devices can provide patients with direct access to their healthcare data, allowing them to analyze and improve their health. Similarly, the work presented by Nayyar et al. (2019) proposed an IoMT-based Health Monitoring (IoMT-HM) framework to analyze the oxygen level, heart rate, and temperature of the patient in real-time.

### **1.3.1.2 Ambient Assisted Living (AAL)**

IoMT technologies are used by AAL to monitor the daily activities of patients, detect health issues, and manage emergencies (Patel and Shah, 2021). These tools are



**Figure 1.3.** *Medical wearable devices.*

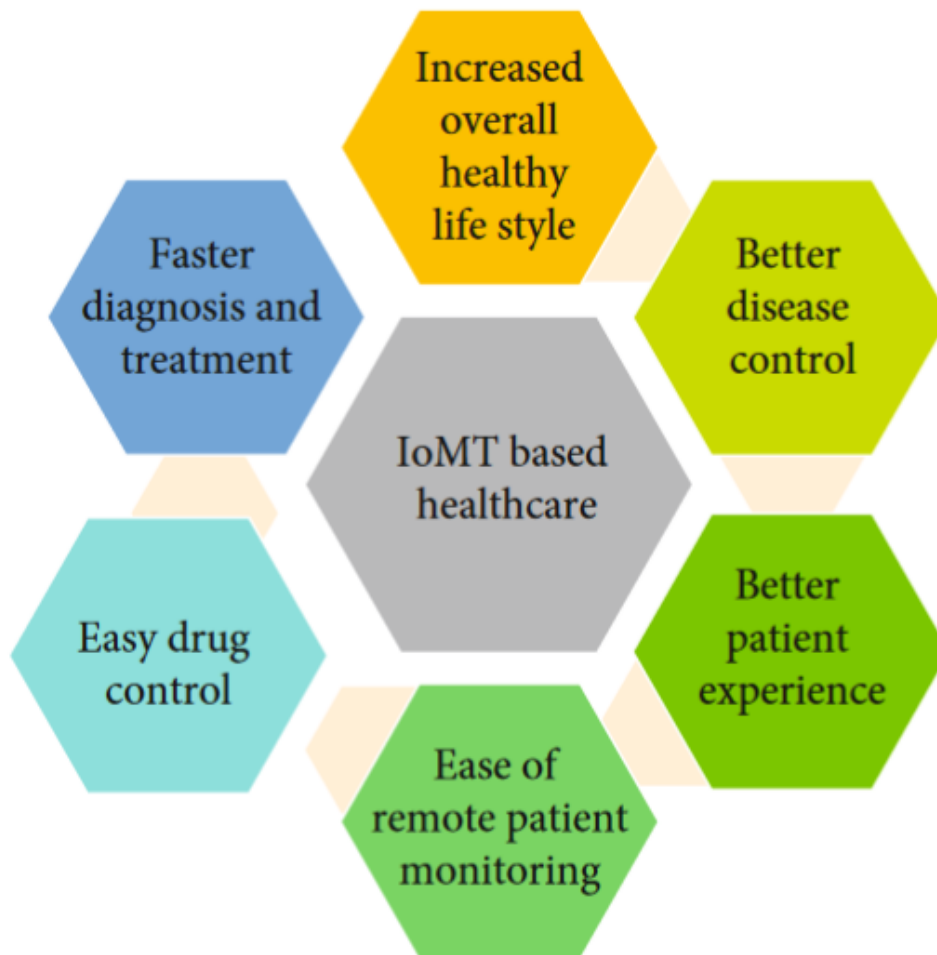
integrated into the patients' homes in an intelligent way to improve the quality of life and reduce healthcare costs. Patel and Shah (2021) proposed the "Keep In Touch (KIT)" technology in AAL, which merged smart items and technologies including RadioFrequency IDentification (RFID) and Near-Field Communication (NFC) to efficiently analyze healthcare data collected from the patient's sensors. Also, to provide the elderly with assistance, Loza-Matovelle et al. (2019) presented an AAL system by combining the sensor network with robotic technology.

### 1.3.1.3 Mobile devices

Generally, mobile devices act as a gateway for communication between patients, hospitals, and medical authorities, in an IoMT-based system. They preserve the patient's health information and allow access to this information by healthcare providers. The devices' portability and accessibility may be the reasons for their enormous popularity. In this field, Saraubon et al. (2018) have developed a smart geriatric care system that uses IoMT and mobile devices to monitor heart rate, detect falls, and provide real-time video monitoring. In another research, Saidi et al. (2019) presented an aging-friendly real-time fall detection system using acceleration values and angular velocity generated by the mobile device's accelerometer and gyroscope sensors.

### 1.3.2 IoMT applications in e-health systems

In the current world scenario, remote healthcare, monitoring a daily healthy lifestyle and telemedicine have gathered particular attention in disease prevention. The benefits of IoMT has been described in Figure 1.4.



**Figure 1.4.** *Benefits of IoMT*

According to Figure 1.4, we can identify some groups of IoMT applications based on monitoring types:

- *Patient monitoring at hospitals:* IoMT applications can be used by patients who are hospitalized, ranging from bed monitoring to more complex applications (Saidi et al., 2019).



- *Patients monitoring in daily activities:* IoMT applications that monitor patients during their daily activities are commonly used by patients that need constant monitoring of their vital signs, such as blood pressure and heart rate. For example, (Vargheese and Viniotis, 2014) proposed an application where daily follow-up of patients is performed 30 days after their discharge from the hospital to avoid the recurrence of the patient with the same problem.
- *Respiratory disease monitoring:* These IoMT applications are used by patients who need to use oxygen cylinders due to chronic respiratory diseases (Masip-Bruin et al., 2016a).
- *Elderly monitoring:* These IoMT applications are used by the elderly for daily activity monitoring. For this reason, authors in (Matsui and Choi, 2017) present a solution to avoid the thermal shock that is one of the biggest causes of death of the elderly in Japan.
- *Human fall detection:* These IoMT solutions can utilize a variety of data sources, including body sensors, accelerometer and gyroscope data, pictures, videos, and so on to detect human falls (Saidi et al., 2019). After the fall detection, an alert is generated and sent to the patient's contacts (family members, caregivers, or medical staff).
- *Improved Drug Management:* IoMT-based RFID tags can manage drug availability issues. Casciaro et al. (2020) have suggested an IoT-based smart pill dispenser for monitoring the elderly's medication regime. In this situation, a mobile application has been developed to notify the elderly and caregivers in case of a wrong medication schedule. Also, Airehrour et al. (2018) have developed a reminder aid system that may send text messages and e-mails to remember the patients about their medication schedule.
- *Emergency Healthcare Service:* Due to the IoMT technology, it is possible to use emergency services from home. These services are a crucial component of

any healthcare service because they address severe and unpredictable health complications like accidents, falls, and heart attacks (Sahu et al., 2021). Several kinds of research have been published on these systems. For example, Korzun et al. (2015) suggested digital help services for emergency cases. According to Eichler et al. (2017), an integrated emergency system is required using more sensors (such as heart rate monitors and blood pressure) and new services to diversify the features and advantages of healthcare.

## 1.4 E-health applications using F2C computing

According to human development's history, e-health applications are the primary driving force behind technological development. Indeed, the adoption of cloud and fog technologies is required to improve e-health systems and solve different challenges. In this context, Manocha and Singh (2022) suggested a new edge analytics-assisted approach to analyze the kinds of Motor Movements (MM) used by the patients in their daily routine. The limiting factors of this system are redundant data elimination and the lack of resource scheduling at the fog-cloud level. Also, Manocha et al. (2020) presented a health monitoring framework based Fog-Cloud computing to evaluate the severity of Generalized Anxiety Disorder (GAD). This technique monitors several environmental and physical factors to analyze health vulnerability. However, this framework has limited accuracy in resource allocation at the fog level.

### 1.4.1 F2C-based e-health architectures

Figure 1.5 demonstrates the architecture of the F2C computing-based e-health systems. This architecture is composed of three layers: the Cloud layer, Fog layer, and IoT devices layer. Generally, sensors (IoT devices) produce medical data continuously and send them to the gateway. The gateway transmits this data to the fog layer where the data can be pre-processed, guaranteeing a rapid response if any emergency is



so that match between provided service, requirements of latency and real-time applications. Additionally, it minimizes the amount of data that is sent from IoT devices to the cloud, instead of storing all data directly in the cloud, temporary data is available to the users through the fog, these data can also be filtered and pre-processed at the fog layer before forwarding it to the cloud.

In summary, F2C benefits for e-health systems (Sinaeepourfard et al., 2017) are as follows:

- Real-time data access.
- Reduce network load by avoiding remote data access and using data available at the fog layer.
- Reduce the volume of data by performing data aggregation techniques.
- Adjust the frequency of the data transmission to use the network in periods when the traffic load is low.
- Provide more accuracy and precision from the sensed data at no additional cost.
- The probability of communication failure and the security risks are reduced as well, so privacy is improved (Sinaeepourfard et al., 2017).

### **1.4.3 F2C data management-based e-health systems**

The distributed hierarchical F2C offers an interesting framework for data management. To ensure effective data management in the F2C-based e-health system, several steps can be followed: data acquisition, data processing, and data storage (Sinaeepourfard et al., 2017).

The IoMT devices layer is primarily responsible for data acquisition. The fog layer can handle basic data processing and storage tasks and the cloud layer is in charge of more complex data processing of big data, as well as permanent data storage. In the following subsections, we detail each step.

### 1.4.3.1 Data acquisition

Data acquisition is mainly performed by IoMT devices. As long as data are being collected, other phases can also be performed at the IoMT devices layer like the data filtering phase which is used to remove redundant data and apply data aggregation techniques to reduce the amount of data to be managed (Sinaeepourfard et al., 2017). Information collected by IoMT sensors is regularly sent to the fog layer and then to the cloud level, where it is stored for historical purposes.

### 1.4.3.2 Data processing

Data processing can be performed at any layer from the F2C hierarchy, according to the requirements of the application. For example, real-time or critical data will be executed at the fog layer to have faster access to the real-time data. Alternatively, computing complex applications will be executed at the cloud layer. In cloud computing, the resources are unlimited and the data set of a high-performance computing application will presumably be very large (Sinaeepourfard et al., 2017).

### 1.4.3.3 Data storage

Data are created by the IoMT devices, sent to the fog layer, and then transmitted to the cloud layer, where they will be permanently stored in “main memory”. Thus, the F2C hierarchy acts as a reversed memory hierarchy, where data are preserved temporarily at the lowest level (fog layer), and provides real-time applications with fast access to these data. In addition, this model can decide the amount of temporal data that will be stored at this level, as well as the frequency of updating to upper levels (Sinaeepourfard et al., 2017).

## 1.5 F2C-IoMT System

Numerous healthcare organizations have implemented IoMT technology with success to achieve goals like smart healthcare monitoring and quick results delivery. However, the storage, processing, and management of health-related data are a significant challenge for the healthcare system regarding the large amount of data generated by IoMT devices. Therefore, to resolve these issues, the integration of F2C computing can support healthcare in realizing the remote patient health monitoring system, it provides accessibility, scalability, and storage capacity, with low costs.

Thus, the F2C-IoMT framework provides better management, monitoring, flexibility, decision services, and agility for e-health systems. These features save cost and energy and help improve reliability (Mohamed et al., 2021). Also, F2C-IoMT provides many capabilities to enable control and communication between patients and healthcare providers to improve the sustainability and resilience of the medical network's infrastructure, data efficiency, and robustness by using system self-management (Mohamed et al., 2021).

The major challenges of F2C-IoMT system can be summarized as follows:

- Security and privacy issues,
- Real-time processing of big data,
- Managing the heterogeneity.

## 1.6 Summary

In this chapter, we provided the fundamentals of e-health, IoMT, and F2C technologies. We have also presented the benefits and advantages when combining IoMT, fog, and cloud computing which offer a robust environment for e-health systems.

Unfortunately, there is an evident requirement for new security strategies able to handle all components in the F2C architecture. In the next chapter, security and privacy concerns and requirements are discussed in a comprehensive and detailed manner.

Chapter

**2**


---

# Security and Privacy issues in E-health systems

---

## Contents

|            |  |           |
|------------|--|-----------|
| <b>2.1</b> | <b>Introduction</b>  | <b>28</b> |
| <b>2.2</b> | <b>Security and privacy goals and concerns in e-health systems</b> | <b>28</b> |
| <b>2.3</b> | <b>Security issues in e-health based F2C-IoMT systems</b>          | <b>29</b> |
| 2.3.1      | Basic security consideration in the F2C system                     | 30        |
| 2.3.2      | Security requirements in IoMT Systems                              | 30        |
| 2.3.3      | Security challenges and directions in the F2C-IoMT system          | 32        |
| 2.3.4      | Most potential attacks in the F2C-IoMT system                      | 34        |
| <b>2.4</b> | <b>Privacy issues in e-health based F2C-IoMT systems</b>           | <b>35</b> |
| 2.4.1      | Privacy: A crucial parameter                                       | 36        |
| 2.4.2      | Privacy Requirements in e-health systems                           | 41        |
| <b>2.5</b> | <b>Related works</b>   | <b>42</b> |
| 2.5.1      | Centralized-based approaches                                       | 42        |
| 2.5.2      | Distributed-based approaches                                       | 43        |
| 2.5.3      | Trusted Third-Party approaches                                     | 45        |
| <b>2.6</b> | <b>Summary</b>   | <b>46</b> |

---

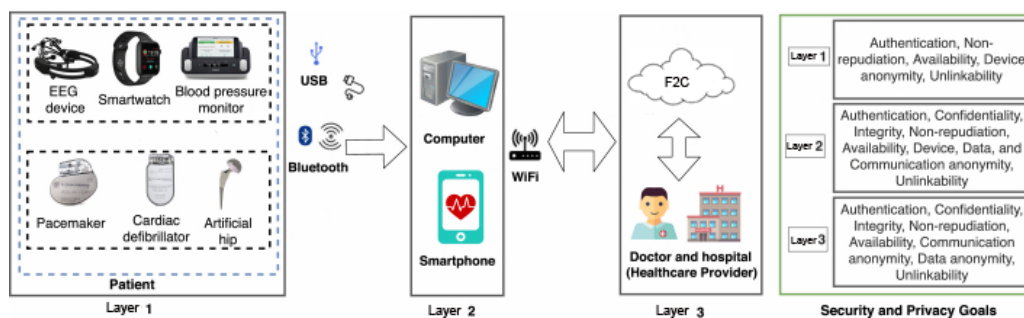


## 2.1 Introduction

In this chapter, we dive through the security and privacy issues that are emerging as challenges against a successful F2C-IoMT deployment. We give a large literature review of the most recent related works and also draw important concepts to bring solid knowledge for the security and privacy schemes that are going to be proposed.

## 2.2 Security and privacy goals and concerns in e-health systems

Several IoMT devices can be placed on the patient's body to monitor the environmental parameters (e.g., ambient temperature and humidity) and the body's vital signs (e.g., blood pressure and ECG signal). As illustrated in Figure 2.1, the e-health system's architecture can be divided into three layers. Before transmitting any patient data, users must be strictly authorized at each layer. Confidentiality and integrity should also be ensured at layers 2 and 3. Additionally, communication between patients and healthcare professionals should be untraceable to achieve anonymity and unlinkability.



**Figure 2.1.** Security and privacy goals in healthcare systems

Due to the conceptual and methodological similarities between privacy and security, many researchers usually presented them as the same thing. Indeed, privacy aims to make appropriate decisions about collection and processing of personal data, whereas security aims to protect and control data (O'Connor et al., 2017). The table 2.1 illustrates the key differences and characteristics of security and privacy challenges.

**Table 2.1.** *Security and privacy characteristics open challenges*

| <b>Security Challenges</b>  | <b>Privacy Challenges</b>  |
|---|--|
| Security addresses confidentiality, integrity, and availability issues. | Privacy addresses personal data.   |
| Security is based on Encryption and decryption algorithms.              | Users cannot use data without permission access.   |
| Provide data confidentiality.   | Preserve data confidentiality. Decide how, what, with whom and if the information is shared. |

The following is a summary of general security and privacy concerns in e-health systems:

- According to the legislation, all data must be properly collected, analyzed, and then stored (O'Connor et al., 2017).
- All data must be used with an adequate level of security and privacy protection (O'Connor et al., 2017).
- All sensors must be able to send and receive data without compromising data integrity and accuracy (Khader and Subasri, 2020).
- All devices must be configured to guarantee adequate protection against specific attacks, unauthorized access to the system, and unauthorized use.

### 2.3 Security issues in e-health based F2C-IoMT systems

Achieving security in e-health is very vital. For that reason, many researchers have suggested a variety of security techniques to ensure and enhance the security of patients' sensitive data. However, if the e-health systems are not secured, the consequences will be catastrophic for the patient's life and the economy. This can happen due to the different types of attacks that may be launched against the networks.

For instance, the Health Insurance Portability and Accountability Act (HIPAA) had put forward by the United States (US) Congress in 1996 as a federal law that applies to the US healthcare industry (HiPAA, 2010).

### 2.3.1 Basic security consideration in the F2C system

In the F2C system, distributed fog nodes act as distributed managers to provide computation, networking, and storage closer to users. To prevent passive and active attacks like man-in-the-middle, the distributed fog nodes and cloud must securely communicate (HiPAA, 2010). Thus, some steps are required to guarantee security across the fog and cloud layers as illustrated in Figure 2.2. To preserve the confidentiality and integrity of data, each fog node must first be securely discovered before performing mutual authentication with the cloud by submitting identities and credentials. The cloud gives fog nodes keys after performing authentication. These keys can be used by fog nodes to encrypt and decrypt information exchanged with clouds, preventing unauthorized parties from altering or deleting the exchange (Al Hamid et al., 2017).

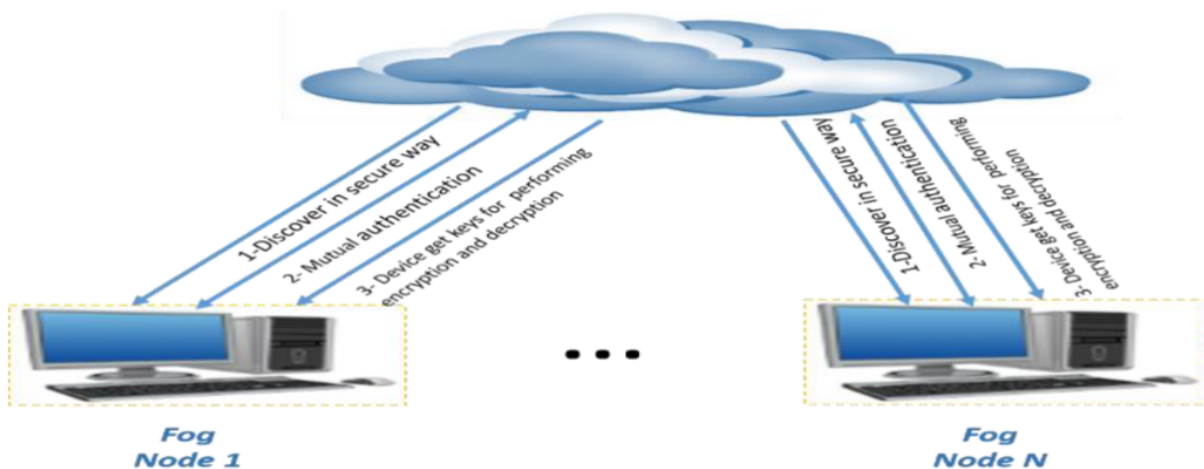


Figure 2.2. F2C layer security

### 2.3.2 Security requirements in IoMT Systems

For effective use of e-health, a set of important security and privacy requirements must be implemented using HIPAA regulations (HiPAA, 2010), which are presented in the table 2.2.

**Table 2.2.** *Security and privacy requirements as recommended by HIPAA*

| <b>Requirement</b>    | <b>Description</b>  |
|-----------------------|---|
| Patient understanding | signifies that individuals have a special right to understand how their private and sensitive medical data are used by any healthcare provider.   |
| Patient control       | Allows patients to choose who can access their medical information.   |
| Confidentiality       | Medical data should be preserved by individuals who should not have access to ensure the confidentiality of data.   |
| Data integrity        | guarantees that any modification or omission of medical data is completely prohibited.  |
| The consent exception | states that the patient's data could be used without his permission only in emergency cases.  |
| Non-repudiation       | A health professional should reject performing a specific activity on a patient's sensitive data.   |
| Auditing              | To ensure that data is effectively secured and preserved, it is necessary to regularly monitor health data along with any other type of activity. This will enable the individual to know whether his info is confidential. |

In general, we can summarize the main security requirements in the following sub-section (Yu et al., 2020), as shown in Figure 2.3.

- *Authentication and authorization:* Fog nodes must offer an authentication method for IoMT devices in the F2C system since they require computational power to perform cryptography and authentication.
- *Access control:* Due to the limited capabilities of IoMT devices, fog layers must offer a distributed access control mechanism for IoMT devices.
- *Confidentiality:* The medical big data generated by IoMT devices must be secured. To ensure that only authorized users and devices can access the medical data which must be encrypted before the transmission process.
- *Identity management:* The main issue in the F2C infrastructure is the enormous number of distributed devices. Thus, techniques for identity management and authentication should be defined, and each device needs to have a unique identity, which must be secured from unauthorized users (Sadique et al., 2020).

- *Integrity*: It offers trusted and accurate information between IoMT devices, fog nodes, and the cloud.
- *Availability*: The IoMT devices and network must be accessible and operate properly without bugs, interruption, or possible problems.
- *Privacy*: IoMT devices can also capture confidential personal information from body sensors. Because IoMT devices have less powerful computational power, various layers in the F2C system must be capable to provide data privacy protection to those devices.
- *Scalability*: Traditional security schemes confront scalability challenges due to the growing number of IoMT devices. To handle this high amount of IoMT devices, the F2C system requires a new scalable security scheme.
- *Cryptographic security*: Fog nodes must provide appropriate cryptographic mechanisms for IoMT devices because they are limited in their capabilities.
- *IoMT devices physical security*: Each device must include a resilience mechanism so that if one is compromised, it won't affect the others. Hence, fog nodes must detect and disable compromised devices.
- *Traceability*: The traceability of the messages is also necessary at any given time. Furthermore, this requirement should be preserved for authorized users.

### 2.3.3 Security challenges and directions in the F2C-IoMT system

The integration of IoMT, fog, and cloud computing into e-health systems has contributed to broad changes in privacy and security protocols, requirements, and healthcare systems. Nonetheless, the following challenges must be considered and addressed in the F2C-IoMT system.

- *Heterogeneity*: The diversity of devices, servers, operating systems, services, platforms, and so forth causes compatibility issues (Shewale and Sankpal, 2020).



**Figure 2.3.** Basic security requirements related to e-health systems

- *Performance:* Each user needs customized applications for his specific objectives based on the requirements, performance, location, etc. (Shewale and Sankpal, 2020).
- *Reliability:* A less complicated mechanism with lightweight components is more reliable than a complex mechanism with many components. Thus, when used independently, IoMT devices, fog, and cloud computing, systems are more reliable. If they are combined into an F2C-IoMT-based system, immense precautions are taken to ensure their operational reliability (Cha et al., 2018).
- *Big Data:* Depending on the volume and complexity of big data, the efficient transmission, storage, access, and processing of big data may not be easily achievable without a combination of IoMT, fog, and cloud systems (Cha et al., 2018).

- *Monitoring*: Continuous monitoring of available resources, equipment failures, and security concerns are crucial for fog and cloud computing system supervision (Saidi et al., 2020).

### 2.3.4 Most potential attacks in the F2C-IoMT system

The F2C infrastructure has several security vulnerabilities, allowing attackers to launch attacks in different layers of the system. Attackers can gain network control of IoMT devices, fog nodes, and cloud-based services to either eavesdrop on communications, change data, or even introduce malicious data into the system. In this section, we identify the most potential attacks to be faced by F2C systems as illustrated in Figure 2.4.

- *Man-in-the-middle attack*: Attackers can even conduct a man-in-the-middle attack by pretending to be a fog node or even a cloud service. They can launch the attack in passive mode (without changing information) or active (information modification, manipulation, and malicious injection) mode, as shown in Figure 2.4.A. This type of attack affects the integrity and confidentiality of any F2C-IoMT system.
- *Denial of service and Distributed denial of service (DoS and DDoS)*: Attackers can launch multiple service requests to the fog nodes or perform a jamming wireless communication between fog node and IoMT devices to deplete the fog node resources and consequently make it down, as illustrated in Figure 2.4.B. An attacker can use legitimate devices, such as IoMT devices or fog nodes to launch DoS and DDoS using their identities. Moreover, DoS and DDoS attacks can also occur in the upper layers. In short, this attack severely affects the availability of the F2C-IoMT system (Bhushan et al., 2017).
- *Database attacks*: In the F2C system, databases may meet a hierarchical architecture, keeping for example one centralized in the cloud and some other

distributed at fog layers. If an attacker can access these databases, it can modify, manipulate and even leak the data, which may have a high impact on the total system performance, as demonstrated in Figure 2.4.C. Database attacks may be internal, coming from F2C services, or external, coming from legible and illegible users. This attack intensely affects the F2C-IoMT integrity and confidentiality (Malik and Patel, 2016).

Thus, proposing a security solution for the F2C framework requires a strong background on possible attacks in each layer and security aspects in the cloud, fog, and IoMT devices.

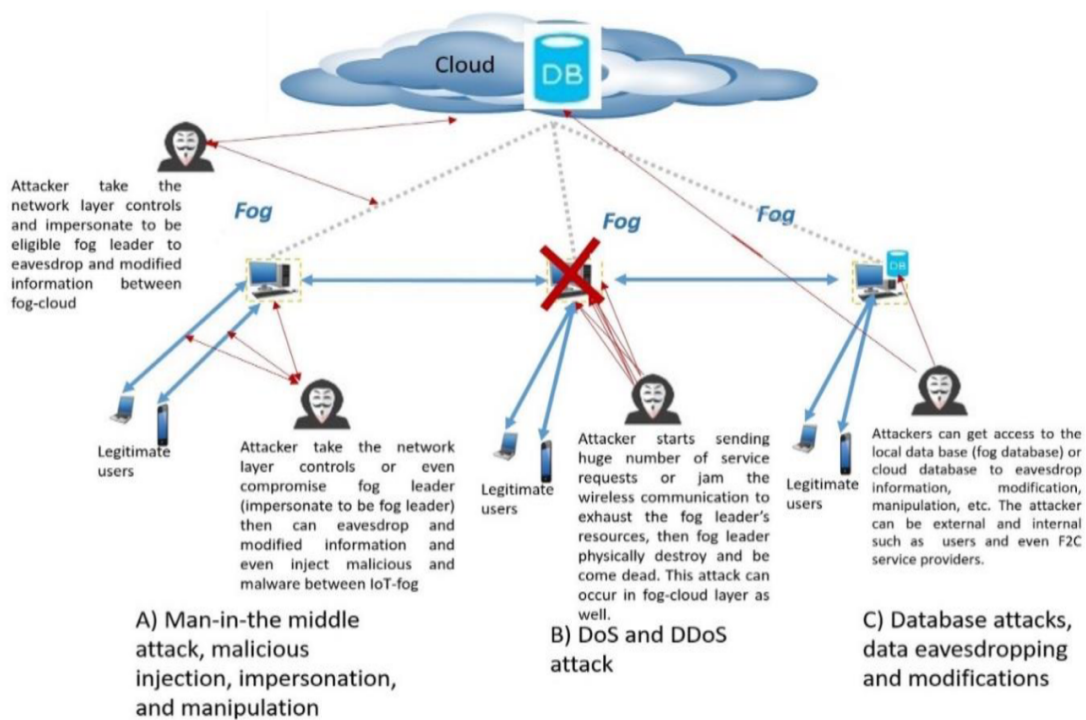


Figure 2.4. Most potential attacks in F2C systems

## 2.4 Privacy issues in e-health based F2C-IoMT systems

The security of personal data, or data privacy, is the most critical element of the healthcare system. Therefore, data privacy is defined as the method through which personal information is protected from unauthorized manipulation, use, or disclosure. Various research studies have therefore been done to identify and define constituent



elements of IoT, fog, or cloud systems and address the critical issues related to data privacy (O'Connor et al., 2017).

### **2.4.1 Privacy: A crucial parameter**

Privacy is one of the most critical security requirements. There are several universally accepted definitions of privacy. According to Clarke (2006), four dimensions are considered to describe privacy. First, personal data privacy requires permissions to control how, when, where, and to whom data are shared. The second dimension is personal privacy which includes the right to control the integrity of the body including medical devices. The third dimension is personal behavior privacy which involves the right to keep any knowledge of the activities and choices private. The final dimension is communication privacy which involves the person's right to communicate without monitoring or surveillance. Whereas, the privacy of personal information is the most addressed dimension by privacy laws [39]. As a consequence, the privacy of personal data is preserved using a variety of techniques, including access control, data anonymization, robust utilization of protocols, and utilizing big data analysis to identify suspicious behavior. In this section, we will review the concept of privacy and define some analysis criteria for comparing privacy-preserving methods in the literature. These criteria are based on privacy regulations, privacy design strategies, and privacy-preserving architectures.

#### **2.4.1.1 Some Privacy Laws and Regulations**

Confidentiality and privacy of patient data managed by healthcare systems should be supported by the law. Unfortunately, most countries have just started to adopt significant laws and give serious thought to policy issues. For example, The Health Insurance Portability and Accountability Act (HIPAA) was adopted in the US in 1996 (HiPAA, 2010). The HIPAA Privacy and Security Rules (HiPAA, 2010) are the most well-known set of regulations regarding privacy in the healthcare domain. It aims

to define significant privacy rights and security policies and ensure portability and accountability among healthcare providers and insurers. In addition, HIPAA covers only those entities that provide healthcare (e.g., hospitals, clinics, and doctors) or handle payment (e.g., insurers), but not other entities such as business associates. Later, HIPAA was extended under the American Recovery and Reinvestment Act (ARRA) (Steinbrook, 2009), in February 2009. ARRA offers the idea for broad deployment of EHR, encourages physicians and hospitals to use EHR, and imposes more privacy protections. According to ARRA, patients have the right to obtain an electronic copy of their data and transmitted it securely to a healthcare provider of their choice. Also, ARRA prohibits the unauthorized use of medical records; it notifies patients of security breaches if their data is affected. In general, the laws and regulations regarding health information privacy differ across providers and regions. Indeed, most European countries have data protection and privacy laws. In the UK, for example, the National Health Service (NHS) is building out a national-scale system of electronic health records (Hewison and Morrell, 2014), basing its privacy practices on the EU Data Protection Directive. Afterward, the EU Data Protection Directive became an important component of EU privacy law. Furthermore, Law 18-07, an Algerian data privacy law, establishes the legal framework for the collection, processing, storage, and disclosure of personal data.

#### **2.4.1.2 Privacy design strategies**

Improving the overall privacy-friendliness of IT systems is the goal of the system design philosophy known as "privacy by design". Thus, privacy requirements must be taken into account throughout the entire system development process, according to the core idea of privacy by design (Hoepman, 2014). Eight privacy design methods were established by Hoepman (2014) from the privacy framework [ISO/IEC29100, 2011] (IEC, n.d.), data protection laws [GDPR, 2016] (Regulation, 2016), and privacy guidelines [OECD, 1981] (Gassmann, 1981). These approaches are described below:

- *Minimize*: The quantity of personal information that is collected, stored, and shared should be minimized as much as possible. This method can be applied by selecting a subset of the incoming data, anonymizing it, and using pseudonyms.
- *Hide*: Any personal information should be hidden. This concept matches the data minimization legal principle. Thus, this strategy is implemented by differential privacy (Mivule, 2013), anonymization and pseudonyms techniques to achieve unlinkability. In other cases, this strategy intends to hide the information from other parties except the legitimate party.
- *Separate*: Personal data should be processed in a distributed environment, in separate sections. This concept recommends using distributed data storage and processing instead of centralized solutions.
- *Aggregate*: The highest level of aggregation and the lowest amount of detail should be used to process personal data. This strategy can be implemented by K-anonymity, l-diversity, and t-closeness (Li et al., 2006). It also matches the data minimization legal principle.
- *Inform*: When processing personal data, data owners should be properly notified. The notifications indicate which data is processed, why, and under what conditions. This strategy matches the transparency, right to access, and breach notification legal principles.
- *Control*: Data owners should be given the appropriate tools to manage their personal information. To give the data owner access to view, delete, and correct personal data, data protection rights must be implemented. This strategy matches the right to access and data portability legal principles.
- *Enforce*: A privacy policy that complies with legal standards needs to be in place and applied. Access control is one such technical protection that must be in to prevent violations of privacy laws. This strategy matches the purpose limitation, data quality, right to be forgotten, and information security legal principles.

Table 2.3. Privacy design strategies

|                    | Data minimization | Purpose limitation | Data quality | Transparency | Right to access | Breach notification | Data portability | Right to be forgotten | Information security | Accountability |
|--------------------|-------------------|--------------------|--------------|--------------|-----------------|---------------------|------------------|-----------------------|----------------------|----------------|
| <b>Minimize</b>    | X                 |                    |              |              |                 |                     |                  |                       |                      |                |
| <b>Hide</b>        | X                 |                    |              |              |                 |                     |                  |                       |                      |                |
| <b>Separate</b>    |                   | X                  |              |              |                 |                     |                  |                       |                      |                |
| <b>Aggregate</b>   | X                 |                    |              |              |                 |                     |                  |                       |                      |                |
| <b>Inform</b>      |                   |                    |              | X            | X               | X                   |                  |                       |                      |                |
| <b>Control</b>     |                   |                    |              |              | X               |                     | X                |                       |                      |                |
| <b>Enforce</b>     |                   | X                  | X            |              |                 |                     |                  | X                     | X                    |                |
| <b>Demonstrate</b> |                   |                    |              |              |                 |                     |                  |                       |                      | X              |

- *Demonstrate*: A data controller must be able to demonstrate that the privacy policy and any other applicable laws are being followed. The demonstrated technique can be implemented through the use of logging and auditing. This strategy matches the accountability legal principle.

In short, to evaluate the privacy-preserving approaches, the eight privacy design strategies can be used. They are listed in Table 2.3 with the legal principle they address. Each privacy legal principle is matched by at least one of the design strategies. Hence, to preserve the data owner’s privacy and prove the privacy legal requirement compliance by the data consumers, the privacy design strategies must be applied by both the data owners and the data consumers. Hence, we split these strategies into a three-layered privacy model in the following section.

**2.4.1.3 Three-layered privacy model**

Protecting privacy is a collaborative process that necessitates the participation of all the involved parties to secure the handled data during the phases of data collection, transmission, storage, and processing. According to Spiekermann and Cranor (Spiekermann and Cranor, 2008), we can distinguish three areas where privacy needs

to be preserved, namely the user sphere, joint sphere, and recipient sphere. In this context, we split the privacy design strategies on the three-layered privacy model, as below:

- *User Sphere*: In this area, the user's devices and data are fully controlled by their owner. Reducing data locally in the user sphere can improve privacy preservation. Thus, applying the first four privacy design strategies, which minimize, hide, separate, and aggregate before outsourcing the data from the owner's control area is more efficient.
- *Joint Sphere*: The user's data are maintained by a third party that offers services like email. The control over the user's data is shared by the data owner and the data consumer. In this area, all privacy design techniques must be used. Thus, the first four privacy design strategies are adopted by the data owner, whereas the last four are adopted by the data consumer.
- *Recipient Sphere*: In this area, the user's data are out of the owner's control because they are sent to a third party which is the only controller. Hence, the data consumer can prove its privacy legal requirement compliance to the data owner or the data controller by adopting the last four privacy design strategies: inform, control, enforce, and demonstrate.

#### 2.4.1.4 Privacy-preserving architectures

To preserve privacy, three types of architecture can be used: centralized, distributed, and third-party architectures.

- *Centralized architecture*: This necessitates a local central node that is located in the user sphere to protect the privacy of the data before it becomes out of the data owner's control. The fundamental issue with this architecture is that all the computation tasks are managed by a single server. Thus, the data owner's privacy can be threatened in the case of server hacking.

- *Distributed architecture*: To secure the privacy of the network's data, all the involved entities must collaborate. Although this architecture overcomes the single point of failure, malicious entity intrusion arises because any entity can connect with any other entity at any time.
- *Trusted Third-Party architecture*: This requires a third party that can be trusted to protect privacy during data collection, transmission, storage, and processing. This third party may be a fog node, a cloud provider, or a data collector. The fundamental issue with such architecture is that it gives full trust to the third party for the whole data protection.

#### **2.4.2 Privacy Requirements in e-health systems**

Privacy has an immense interest in e-health care because the improper use of EHR and illegal disclosure can cause legal challenges and damaging consequences to people's lives (Khader and Subasri, 2020). In fact, according to Mohandas (2014), privacy in an e-health environment has to be maintained by the following requirements:

- *Anonymity*: is necessary when the EHR identifying information requires to be hidden from other parties. These parties can include management staff, researchers, insurance providers, and any user who has no appropriate access rights. However, physicians and nurses, delegated healthcare providers, and emergency medical technicians (EMTs) should be able to examine such information to give proper treatment. In addition, the patient's identity can be deduced from the medical data.
- *Unlinkability*: indicates that multiple EHRs cannot be linked to the same owner. This requirement prevents the profiling of a patient by insurance companies or central servers that store patient data. The unlinkability requirement is applied to the monitor center servers, which has the curious-but-honest assumption, i.e. that the servers will understand the patient's privacy, but will not launch

attacks on the stored EHRs. Anonymity is a prerequisite for unlinkability because identifying information makes EHRs linkable.

- *Minimum disclosure*: IoMT devices transmit medical data where it reveals a certain amount of information. This amount of information must be kept as minimum as possible.

## 2.5 Related works

In this section, we provide a review of the literature on privacy-preserving approaches proposed in the IoT domain. We categorize them based on the three architecture types defined on Section 4.1.4.

### 2.5.1 Centralized-based approaches

Centralized-based approaches rely on one or a few central nodes in which data are stored to preserve privacy before sending the data. Kravets et al. (2015) proposed Incognito, a privacy-preserving IoT framework, where the user can generate a new identity for each given context. Indeed, Incognito protected the users' privacy by providing them full control over the data traces that they leave in an IoT infrastructure.

For their part, González-Manzano et al. (2016) proposed PAgIoT, a Privacy-preserving Aggregation protocol. PAgIoT enabled the aggregation of many attributes for a set of entities while allowing for privacy-preserving value correlation.

In addition, Lu et al. (2017) proposed LPDA, a lightweight privacy-preserving data aggregation scheme based on fog computing-enhanced IoT. LPDA used a one-way hash chain mechanism to allow a fog node to filter false data by performing the source authentication at the network edge. Additionally, LPDA integrates the data from several hybrid IoT devices into a single ciphertext, it consisted of four actors: IoT devices, a fog device, a control center, and a trusted authority. IoT devices periodically

sent the data to a fog device, which aggregated the received data and forwards them to the control center that can perform data analytics on the aggregated data. The trusted authority's role is to assign and manage keys to all the IoT devices, the fog node, and the control center.

To address privacy-preserving data aggregation in the fog-enhanced IoT environment, Guan et al. (2019) suggested a device-oriented anonymous privacy-preserving system with authentication, known as APPA. APPA scheme included five entities: local certification authority, trusted certification authority, smart devices, fog node, and public cloud server. The two authorities are responsible for the system's certification management. Smart devices collected and sent the data to the fog node that stored and aggregated the received data. Then, it transmitted the aggregated data to the public cloud server to process the data.

Allison et al. (2016) proposed a framework that aimed at preserving privacy while collaborating. The proposed framework contained a collaborative privacy manager aimed at assisting collaborating users with their privacy preferences, making decisions, and providing users with knowledge and suggestions.

However, the main issue with the centralized-based techniques is that all the preserving privacy computation tasks are managed by a single node. Thus, in the case of node hacking, all the user's sensitive data are attacked.

## **2.5.2 Distributed-based approaches**

To overcome the single point of failure issue, the distributed-based approaches enabled all the network devices to collaborate among them to protect their data privacy. For big data storage issues, Liang et al. (2015) proposed a privacy-preserving ciphertext multi-sharing mechanism that combines the merits of proxy re-encryption with anonymous techniques to share a ciphertext several times without disclosing both the identity information of ciphertext and the knowledge of the plaintext. Additionally, He et al. (2016) addressed the privacy-preserving data aggregation in ad-hoc networks



by using the distributed consensus method called SCDA (secure consensus-based data aggregation) that guarantees an accurate sum aggregation while preserving the privacy of sensitive data. According to the authors, SCDA could be implemented in a distributed manner and robust against the network dynamics.

According to Froelicher et al. (2017), using a centralized authority to preserve privacy is not an appropriate solution. For this reason, authors proposed a decentralized system, called UnLynx for efficient privacy-preserving data sharing, guaranteeing the confidentiality and the unlinkability between data providers and their data.

More recently, the blockchain has been used as a solution for managing privacy-preserving data. Based on this technique, ProvChain, a trusted and decentralized architecture, was presented by Liang et al. (2017). ProvChain collected and validated the provenance of cloud data by including the provenance data in blockchain transactions.

In the same context, Li et al. (2018) suggested the CrowdBC model, a decentralized platform for crowdsourcing based on blockchain. A crowd of workers can solve a requester's task without relying on any trusted third party while guaranteeing the users' privacy. Recently, blockchain technology has received significant attention. In this regard, Hashemi et al. (2016) proposed a decentralized solution for sharing data in the IoT environment using blockchain to maintain the data access control and the data storage model. The main characteristics of this model are decentralized access control and separation of the data store and data management.

For their part, Hardjono and Smith (2016) presented a privacy-preserving technique for integrating an IoT device into a cloud system. Their new Chain Anchor architecture allows an IoT device to prove its manufacturing provenance without the authentication of a third party and it is allowed to register anonymously through the use of a blockchain system.

Jayaraman et al. (2017) presented a novel technique for the privacy preservation of IoT data, which used several IoT cloud data stores to preserve IoT data privacy. The goal of this model was to decompose the IoT data into chunks, store them in multiple data stores, and re-aggregate them when asked by a user without exposing anything beyond meaningless addends.

In addition, Ouaddah et al. (2016) suggested a novel privacy-preserving technique based on blockchain technology, called FairAccess. The authors extended the functionality of the Bitcoin system and included additional types of transactions to provide access control, including grant, get, and revoke access. Blockchain is used for storing and reading permissions. Furthermore, the framework is based on three actors: the shared resource, the resource owner, and the users. The resource owner controlled the resource accesses through transactions.

Dorri et al. (2017) proposed Blockchain for IoT security and privacy-preserving. They applied a lightweight blockchain for a smart house. In each house, multiple IoT devices (e.g., smartphones, personal desktops, and sensors) are connected to the same network and each house is equipped with a powerful resource device, known as the house's miner to manage all transactions inside the house.

### **2.5.3 Trusted Third-Party approaches**

Traditional security and privacy mechanisms are inadequate for Big Data (Colombo and Ferrari, 2015). In this context, Colombo and Ferrari (2015) proposed an initial step to include privacy-aware access control (PAAC) functionalities into existing big data platforms. They discussed a variety of activities, such as the definition of policy specification, the identification of policies for Big Data platforms, and the definition of enforcement mechanisms.

Similarly, Yang et al. (2015) proposed a solution to share sensitive medical data with cloud computing while preserving the patient's privacy. To take into account various components of medical data with various privacy issues, the medical dataset

is vertically partitioned. Patient identification information is stored in the ciphertext. The remaining components, which will be utilized for medical analysis, are kept in plaintext. Thus, the cloud environment is used as a joint sphere to share medical records.

To summarize, some privacy approaches are classified in Table 2.4.

**Table 2.4.** List of some privacy approaches.

|                           | Architecture        | User sphere  |      |          |           | Joint sphere |           | Recipient sphere |         |         |             |
|---------------------------|---------------------|--------------|------|----------|-----------|--------------|-----------|------------------|---------|---------|-------------|
|                           |                     | Minimization | Hide | Separate | Aggregate | Secure Comm. | Anonymous | Inform           | Control | Enforce | Demonstrate |
| Allison et al. 2016       | Centralized         | X            |      |          |           | X            |           | X                |         | X       |             |
| Liang et al., 2015        | Distributed         |              | X    |          |           |              | X         |                  |         | X       |             |
| Liang et al., 2017        | Distributed         |              | X    |          |           |              | X         |                  | X       | X       | X           |
| Li et al., 2018           | Distributed         |              | X    |          |           |              | X         |                  |         |         |             |
| Yang et al., 2015         | Trusted Third-Party |              | X    | X        | X         | X            |           |                  | X       | X       |             |
| Colombo and Ferrari, 2015 | Trusted Third-Party |              |      | X        |           | X            |           |                  |         | X       |             |

Some of these methods allowed the protection of privacy by trusting a third-party (Yang et al., 2015), (Colombo and Ferrari, 2015), while some other techniques are more distributed and did not require trust (Liang et al., 2015),(Liang et al., 2017),(Li et al., 2018). Additionally, the control mechanism is partially ensured in (Yang et al., 2015) and (Liang et al., 2017) by allowing the data integrity check and proposing a key to decrypt and modify the stored data.

## 2.6 Summary

In this chapter, we have surveyed the security and privacy issues in the e-health domain, especially in the IoMT, fog, cloud, and F2C domains. First, we gave an

overview of the security issues and requirements, then we mainly addressed the privacy concerns that arise as a result of the personal data collection process.

In the next chapter, we introduce the different techniques and mechanisms used to preserve the security and privacy of medical data.

Chapter

**3**

---

# Data security and privacy techniques

---

## Contents

---

|            |   |           |
|------------|---|-----------|
| <b>3.1</b> | <b>Introduction</b>                               | <b>49</b> |
| <b>3.2</b> | <b>Security and privacy-preserving techniques</b> | <b>49</b> |
| 3.2.1      | Restriction-based mechanisms                      | 49        |
| 3.2.2      | Perturbation-based mechanisms                     | 54        |
| 3.2.3      | Aggregation-based mechanisms                      | 56        |
| 3.2.4      | Decentralized-based mechanisms                    | 59        |
| <b>3.3</b> | <b>Related works</b>                              | <b>66</b> |
| 3.3.1      | Encryption techniques                             | 66        |
| 3.3.2      | Access control techniques                         | 67        |
| 3.3.3      | Differential Privacy                              | 68        |
| 3.3.4      | Anonymization/Pseudonymization techniques         | 68        |
| 3.3.5      | Homomorphic encryption techniques                 | 69        |
| 3.3.6      | Blockchain techniques                             | 69        |
| 3.3.7      | Self-Sovereign Identity Technology                | 70        |
| <b>3.4</b> | <b>Summary</b>                                    | <b>71</b> |

---

## 3.1 Introduction

Privacy's definition varies over time, among cultures, and individuals. The first definition of privacy was by Warren and Brandeis (1890), who defined privacy as "*the right to be let alone*". Then, the privacy definition became the ability to control personal data with the emergence of new technologies. Data privacy required ensuring data security and taking into account requirements from both the legal regulations and the individual's preferences (Mohandas, 2014).

This chapter presents introductions to security and privacy techniques which will be helpful to understand the remainder of this thesis. Also, a review of the work-related is discussed. Therefore, in Section 2, we present some privacy-preserving mechanisms before surveying some existing privacy-preserving approaches in healthcare domains in Section 3.

## 3.2 Security and privacy-preserving techniques

To resolve the security and privacy challenges and enhance the security of the patient's health data, security and privacy techniques must be defined (Babaghayou et al., 2023). Thus, based on the overview of security and privacy issues studied in the previous chapter, we survey, in this chapter, some existing security and privacy-preserving techniques. These techniques can be classified into several mechanisms such as perturbation-based mechanisms, restriction-based mechanisms, aggregation-based mechanisms, and decentralized-based mechanisms.

### 3.2.1 Restriction-based mechanisms

Data restriction methods are based on cryptographic and access control techniques.

### 3.2.1.1 Cryptographic protection techniques

The data encryption technique is a vital tool whose value cannot be overstated. It helps protect information from data breaches; it guarantees that no one can read messages or access data except legitimate users or data owners. There are several data encryption approaches. Usually, they are decomposed into three distinct methods: symmetric, asymmetric, and hashing, as shown in figure 3.1.

#### 1. *Symmetric cryptography schemes*

Symmetric cryptography schemes often called private-key cryptography or a secret key algorithm, are a type of encryption algorithm in which the same key is required to encrypt and decrypt data. These methods are characterized by their high efficiency because they do not consume a lot computational time as asymmetric cryptography does. Also, symmetric encryption is faster than asymmetric encryption. However, both parties must ensure that the key is stored safely and accessible only to the necessary software.

#### 2. *Asymmetric cryptography schemes*

Asymmetric cryptography, known as public key cryptography is based on pair of keys mechanism. One key is public, it is accessible to everyone and used to encrypt data or to verify the digital signature. Whereas the second key is the private key, which can only be used by its owner to decrypt the encrypted data or sign it with a digital signature. Both keys are not identical, they are simply large numbers paired with each other, where the “asymmetric” name comes in. Even though asymmetric cryptography provides high efficiency, it also introduces additional overhead and requires big computational processes which do not fit the real-time applications and constraints of an e-health environment.

#### 3. *Hashing techniques*

The hashing algorithm is cryptographic and mathematical scheme. It is a one-way program, so the text can't be decoded by anyone, which means data

encrypted with hashing cannot be decrypted into its original form. For this reason, hashing is used only to validate data.

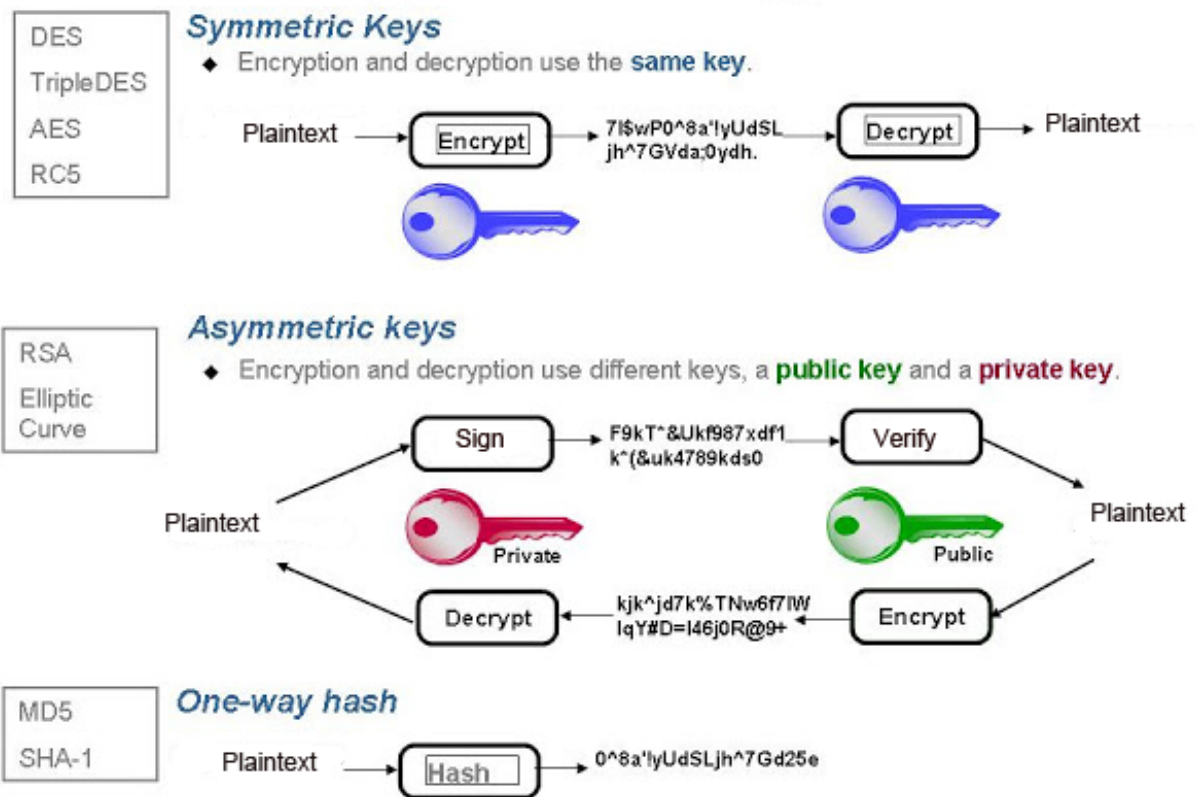


Figure 3.1. Data encryption techniques

### 3.2.1.2 Access Control Techniques

The access control technique can be defined as the formalization of rules for allowing or denying the rights or privileges to a subject concerning an object. Thus, the access control technique aims to check and restrict the actions that authorized users can perform, the restrictions include who can access what data and how others manipulate their shared data. Many access control models exist. They vary in their design, components, policies, and application area.

#### 1. Mandatory Access Control (MAC)

MAC is an access control model where the system grants users access depending on the amount of the information's sensitivity and the user's authorization.



Access is controlled by the administrator and users can't modify security attributes even for their data. In addition, MAC is a hierarchical scheme based on a security level. Users are assigned a security level, and objects are assigned a security label. Thus, users are only permitted to access resources that correspond to their security level or lower.

## 2. *Discretionary Access Control (DAC)*

DAC is an identity-based access control scheme that gives the user a certain level of control over his data. Access permissions are stored in an access control list (ACL), they can be defined for specific users or groups of users by data owners. The list can be created automatically or generated by the administrator when a user allows access to another user. Also, an ACL includes the levels of access that users have.

The main principles of DAC:

- The object's name, size, and directory path are hidden from unauthorized users.
- Additional authentication factors are required in case of several failed access attempts.
- The owner can define the access level of other users.

## 3. *Role-based access control (RBAC)*

RBAC was formally announced by Sandhu et al. (2000). It was initially proposed for enterprises where permissions will be granted to roles rather than individual users. An organization can create roles based on various job functions and responsibilities, and users can be assigned these roles. The idea of roles greatly simplifies the management of permissions because system administrators do not need to manage individuals and their permissions. Roles can be granted and revoked permissions to users of certain applications and systems as necessary. In short, the core notion of RBAC is that users and permissions can be associated with roles, as shown in Figure 3.2.

#### 4. *Organization-based access control (OrBAC)*

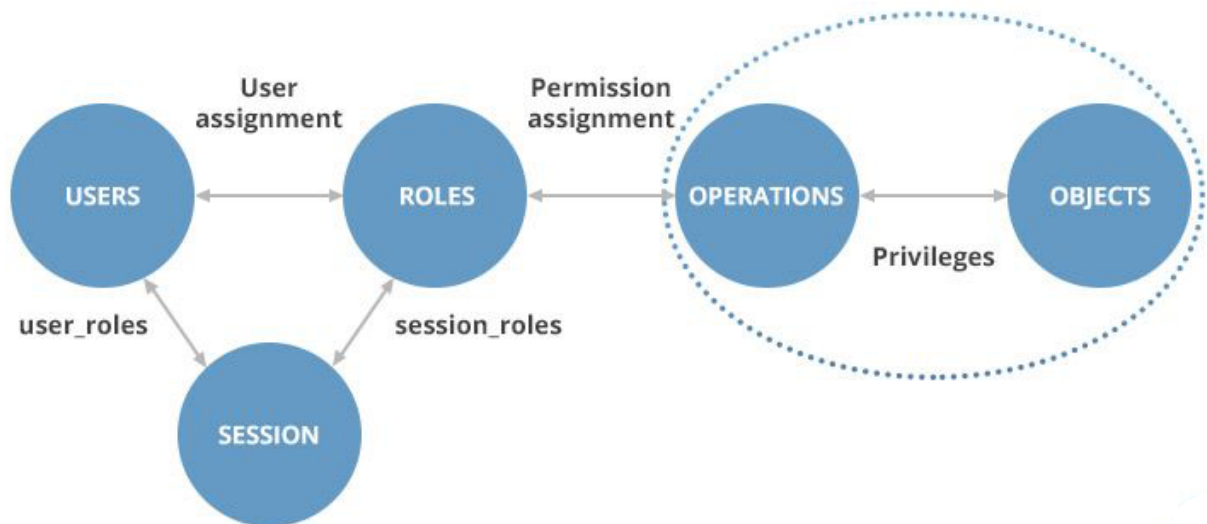
The key concept of OrBAC is the organization that is responsible for managing a security policy. The OrBAC model suggests using the roles of subjects, objects, and actions inside of the organization instead of managing the security policy based on the subject, object, and action concepts. Therefore, OrBAC is based on eight primary sets of entities: organizations (Org), actions (A), subjects (S), objects (O), roles (R), activities (A), views (V), and contexts (C). Each organization should specify roles that have the permissions, obligations, or prohibitions to do some activities in a given context.

#### 5. *Attributed-based access control (ABAC)*

ABAC is described by a logical scheme that evaluates access permissions using conditions against attributes of the object, subject, and environment. Therefore, ABAC supports complex authorization processes and constraints that are defined by the relationship between attributes of physical location, behavior, time, resource types, and other additional information associated with access. In addition, attributes are variable and dynamic, while policies are relatively static. It can also support cases where users are dynamically changing (Brossard et al., 2017).

#### 6. *Centralized and decentralized access controls*

Administration of access control techniques can be decentralized, centralized, or hybrid. A centralized access control manages user authorizations by providing a unified identity inside the organization. The primary problem of centralized access control is the single point of failure. However, decentralized access control allows different entities to grant users access permissions. This approach can be more stable than centralized access control, but it will require more administration and maintenance to protect several entities.



**Figure 3.2.** *Role-based access control (RBAC)*

### 3.2.2 Perturbation-based mechanisms

To maintain privacy, these mechanisms use a variety of methods (Mohandas, 2014) such as noise addition and anonymization techniques.

#### 3.2.2.1 Noise addition techniques

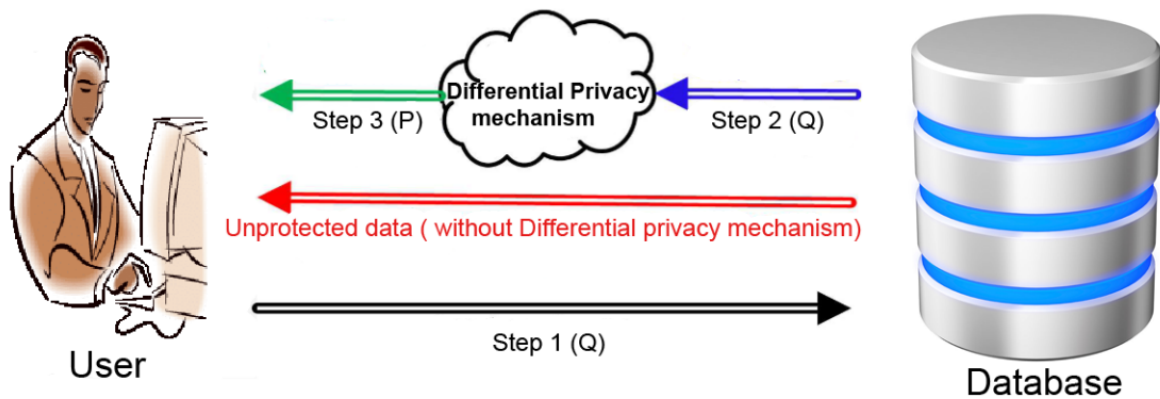
These techniques add noise to the original data to prevent the identification of a particular user (Mivule, 2013). Different techniques exist in this approach; the most popular one is the differential privacy technique which is a powerful tool for solving practical privacy challenges.

1. *Differential privacy technique*

The concept of differential privacy is purely mathematical (Dwork et al., 2006). It consists of adding noise to a query result (Mivule, 2013). The differential privacy challenge lies in determining where to add the noise and how much to add. One of the most commonly used mechanisms for adding noise is the Laplace mechanism (Dwork et al., 2006).

To achieve the privacy goal, more noise must be introduced; unfortunately, this additional noise may make the results less useful. In fact, by adjusting the privacy

parameter ( $\epsilon$ ), also known as a privacy budget or privacy loss, we can regulate the strength of the privacy guarantee. Figure 3.3 illustrates the differential privacy principle. In step 1, the user generates a query  $Q$  and submits it to the private database  $D$ . Step 2, the Private database receives  $Q$  from the user, then sends it to the differential privacy mechanism. Step 3, Differential privacy algorithm adds noise to  $Q$ .  $P$  is the noisy output that will be submitted to the user.



**Figure 3.3.** *Differential privacy technique*

Formally speaking, if we consider a database as a set of rows, we say databases  $D1$  and  $D2$  differ in at most one element if one is a proper subset of the other and the larger database contains just one additional row.

**Definition 1.** A randomized function  $K$  gives differential privacy if for all data sets  $D1$  and  $D2$  differing on at most one element, and all outputs  $S$ ,

$$\Pr[K(D1) \in S] \leq \exp(\epsilon) \times \Pr[K(D2) \in S] \quad (3.1)$$

The loss of privacy is quantified using  $\epsilon$ , which is used to determine the noise addition for ensuring DP. As can be noted, absolute privacy is obtained when  $\epsilon = 0$ . Achieving higher levels of privacy preservation (small  $\epsilon$ ) involves adding more noise to the data which leads to a decrease in the output accuracy of the algorithm and vice versa. In other words, decreasing the parameter means increasing the output accuracy at the cost of loss of privacy.

### 3.2.2.2 Anonymization protection techniques

Anonymization is one of the simple techniques used to protect privacy; it offers minimal computing complexity as compared to other techniques.

Anonymization is based on the removal or change of sensitive attributes such as identification numbers, names, gender, and postal codes. More sophisticated methods such as k-anonymization (Sweeney, 2002), l-diversity (Machanavajjhala et al., 2007), and t-closeness (Li et al., 2006), are employed for strong privacy preservation guarantees.

In the k-anonymity technique, if each value in a given dataset is indistinct from a minimum of (k-1) records from the same dataset, then the dataset is said to be k-anonymous. The greater the k-value, the higher the privacy protection (Sweeney, 2002).

However, due to the background knowledge limitation in k-anonymity, other mechanisms are suggested such as l-diversity which is an extension of k-anonymity. L-diversity is based on the idea that the sensitive attributes in each group are “well-represented” (Li et al., 2006). A dataset has l-diversity if, for every set of rows with identical quasi-identifiers, there are at least l distinct values for each sensitive attribute.

The t-closeness is a further refinement of l-diversity. Thus, an equivalence class is said to be t-close if the distance between its sensitive attribute and the sensitive attribute of the entire table is less than or equal to a threshold (Li et al., 2006).

### 3.2.3 Aggregation-based mechanisms

The goal of data aggregation mechanisms is to release information about the data provided by several users without any information leakage about users' data. Data aggregation methods include zero-knowledge proofs, multiparty computation, and homomorphic encryption-based techniques.

### 3.2.3.1 Zero Knowledge Proofs (ZKP)

ZKP is a mathematical mechanism to check the security of information without disclosing the information itself. It represents the next-generation technology in cryptography, giving users the capacity to verify certain facts about themselves without revealing entire information (Qi, 2009).

The zero-knowledge proof is considered to be a two-party protocol between the 'verifier' and the 'prover' (Yang and Li, 2020), it has the following specification requirements:

- A verifier cannot learn from the protocol because the ZKP requires that zero information is released in any form.
- A prover cannot cheat a verifier, i.e. if failures occur, a verifier is in doubt of a prover's legitimacy.
- A verifying party cannot cheat a proving party.

#### 1. *Properties of ZKP*

ZKP technique must fulfill these criteria:

- **Soundness:** the ZKP technique must enable the verifier to refute the honesty of the prover if the information provided by the prover is false.
- **Completeness:** the ZKP technique must allow the verifier to check that the prover is completely honest and that the information provided by the prover is correct.
- **Zero-knowledge:** the ZKP technique has nothing to disclose to the verifier whether the prover is telling the truth or not.

### 3.2.3.2 Multiparty computation (MPC)

Multiparty computing is a concept that gives different parties to a relationship the ability to share data, do computations, and arrive at a mutual result without divulging

their private data. Moreover, MPC is a cryptographic technique that allows a group of users to compute any function of their private messages while maintaining the privacy of each user's input.

Thus, MPC techniques may enable the coordination of operations and cooperation where it was previously difficult due to a lack of trust. These techniques are effective for ensuring data computation by relying on multiple parties that have to cooperate to get the aggregated result without the involvement of any trusted party (Cramer et al., 2000).

Different solutions of MPC techniques exist, based on logic circuits, arithmetic circuits, or linear secret sharing schemes (Cramer et al., 2000) such as SEPIA (Burkhart et al., 2010) and P4P (Duan et al., 2010).

The characteristics of MPC are:

- Participation of one or several parties (companies or organizations).
- Each party is independent.
- No trust between parties with all their data.
- All parties have access to the same computing and storage platform.
- Certain processes must be kept private for some of the involved parties.

### 3.2.3.3 Homomorphic encryption-based protection

The problem with encrypted data is that we must decrypt it to work with it. Thus, Homomorphic encryption (HE) algorithms are designed to enable operations to be performed on encrypted data. This means that HE makes it possible to analyze or manipulate encrypted data without revealing the data to anyone. However, the problem is that designing the HE algorithm is hard. Different types of this HE algorithm exist:

#### 1. *Partially Homomorphic Encryption (PHE)*

PHE is where only a single mathematical function can be performed on encrypted values, for example, addition or multiplication can be done an infinite number of times. An algorithm is additively homomorphic i.e. that adding two ciphertexts together generates the same result as encrypting the sum of the two plaintexts. PHE with multiplicative operations is the foundation for RSA encryption, which is commonly used in establishing secure connections through SSL/TLS.

#### 2. *Fully Homomorphic Encryption (FHE)*

FHE is capable of using both addition and multiplication any number of times and makes secure multi-party computation more efficient. The goal behind FHE is to allow anyone to use encrypted data to perform useful operations without access to the encryption key. However, these techniques are heavily used when preserving privacy because they enable obtaining computation results over ciphertext calculation without knowing the appropriate plaintexts and private keys of the ciphertexts (Acar et al., 2018). Several homomorphic encryption schemes exist, such as the El Gamal cryptosystem (ElGamal, 1985), and the Paillier cryptosystem (Paillier, 1999). According to Acar et al. (2018), ElGamal cryptosystems are only multiplicatively homomorphic. Hence, it does not allow the homomorphic addition of ciphertexts. However, the Paillier cryptosystem implements additive and multiplication operations.

### **3.2.4 Decentralized-based mechanisms**

To solve the problem related to trusting centralized parties to meet privacy requirements, decentralized methods are adopted for better scalability and reliability. Thus, decentralized solutions have been considered the panacea to privacy issues. To this end, our research is based on decentralized mechanisms such as blockchain and SSI technology.



### 3.2.4.1 Distributed ledger Blockchain

Blockchains are digital ledgers implemented in a distributed environment without a central authority. At their initial level, they enable a community of individuals to register transactions in a shared ledger. The transaction is considered a communication form between network nodes.

Despite the rapid development of blockchain technology and the many variations of blockchain networks, most of them use common core concepts. They consist of several blocks linked together. Each block is composed of a block header and block data. The block header contains the block's metadata and a cryptographic link to the previous block's header (except for the first block of a blockchain), whereas the block data contains a set of transactions and other related data, each transaction is digitally signed by the user who submitted the transaction (Yaga et al., 2019).

#### 1. *Characteristics of blockchain technology*

To illustrate the blockchain's functionality, it is crucial to understand the key characteristics that make up its backbone (Yaga et al., 2019).

- *Decentralization:* A centralized trusted agency, such as the government or a banking institution, must validate each transaction performed by a user on the system. However, these systems may have performance and cost drawbacks, as centralization can result in bottlenecks at a central access point.
- *Persistency:* Transactions generated by users can be validated using the mining process, preventing invalid transactions to be pushed on the blockchain infrastructure. Once a transaction is successfully implemented into the blockchain infrastructure that block can't be deleted, modified, or rolled back.

- *Anonymity*: The blockchain infrastructure enables users to interact using a securely generated address in the form of a hashed value, thus it prevents other users from being able to reveal the identity of users.
- *Auditability*: Different blockchain technologies provide mechanisms for storing and verifying transactions. For example, based on the bitcoin network, data is stored using a user's balance based on the unspent transaction output (UTXO) model (Nakamoto, 2008).
- *Immutability*: Blockchain is append-only database technology, i.e. once the data is recorded into the blockchain, it cannot be possible to manipulate it.
- *Transparency*: It is one of the crucial aspects of the blockchain. Within the blockchain network, anyone can join, participate, and visualize the transactions record. Tracking the movements of digital assets using blockchain technology enables the capability to verify an asset's provenance and authenticity directly. Every node can have a complete and constantly updated copy of the ledger, and it allows them to be used for monitoring.

## 2. Different types of blockchain

Blockchain protocols come in two primary variations: permissionless and permissioned (Helliard et al., 2020). While both permissioned and permissionless blockchains have their benefits and drawbacks.

- *Permissionless blockchains*: are more often referred to as public blockchains due to their open nature so that anyone can join them. With this blockchain type, practically anyone can send and receive transactions, participate in the consensus process, and view, copy and contribute to the code. Some examples of popular permissionless blockchains are Bitcoin (BTC), Ethereum (ETH), Cardano (ADA), and Dogecoin (DOGE) (Singh et al., 2022).
- *Permissioned blockchains*: are more commonly called private blockchains. They are restrictive and required some authority that allowed authorized

accesses, and are typically controlled by a specific user, entity, or group. In addition, the concept of permissioned blockchains is that the problems faced by permissionless blockchains can be avoided by granting access to only trusted users. They are often used by business organizations that desire a secure database with controls. For instance, Hyperledger Fabric is an open-source enterprise-grade and permissioned distributed ledger platform proposed by IBM (Nasir et al., 2018).

### 3. Mining

Miners are specific nodes in the blockchain responsible for collecting transactions, solving challenging computational puzzles (proof-of-work) to reach consensus, and adding the transactions in form of blocks to the distributed public ledger blockchain.

#### 3.2.4.2 Self Sovereign Identity system (SSI)

The SSI is a new paradigm for digital identity, it proposes a new approach by giving users full control of their digital identities without relying on a centralized authority. For this reason, it is called “Self-Sovereign Identity”. To define SSI, we must first define what a digital identity is.

##### 1. *digital identity*

A digital identity is defined as the “unique representation of a subject engaged in an online transaction” by the National Institute of Standards and Technology (NIST) (Grassi et al., 2017). The NIST further states that a digital identity does not necessarily need to uniquely identify the subject in all contexts but it is unique in the context of a digital service. Moreover, a digital identity consists of various types of data, such as identifiers, attributes, and credentials.

- *Identifiers*: Identifiers are random or non-random set of bits that identify entities in a specific context. It is important to note, that the identifier does not have to be universally unique, but only within its context. Furthermore,

an identifier can have at most two of the following properties (Preukschat and Reed, 2021):

- (a) **Human-readable:** Identifiers have semantics in human language.
- (b) **Secure:** Identifiers are unique and thus bound to a single entity.
- (c) **Distributed:** The namespace of the identifier is not managed by any central authority. Identifiers can be generated and resolved independently.

For example user names, domain names and e-mail addresses are human-readable and secure but do not fulfill the distributed criterion. However, this is precisely what is needed for an SSI ecosystem in which users can own and manage their identity in a self-determined and sovereign manner.

- *Attributes:* Attributes are a set of data that collectively constitute the digital identity, for example, a gender, date of birth, or address. Attributes can be declarative or certified. Declarative attributes are declared by the owner of the identity, without proof by other parties, while certified attributes are proven to be valid by a third party (Baier et al., 2010).
- *Credentials:* Credentials are a means to verify identity by containing data about an identity holder, they can be defined as “an identifiable object that can be used to authenticate the holder is what it claims to be and to authorize the holder’s access permissions” (Harrop, 2009). Thus, credentials prove the authenticity of an identifier, and they can be used in different scenarios. NIST categorized credentials into three levels (Grassi et al., 2016):

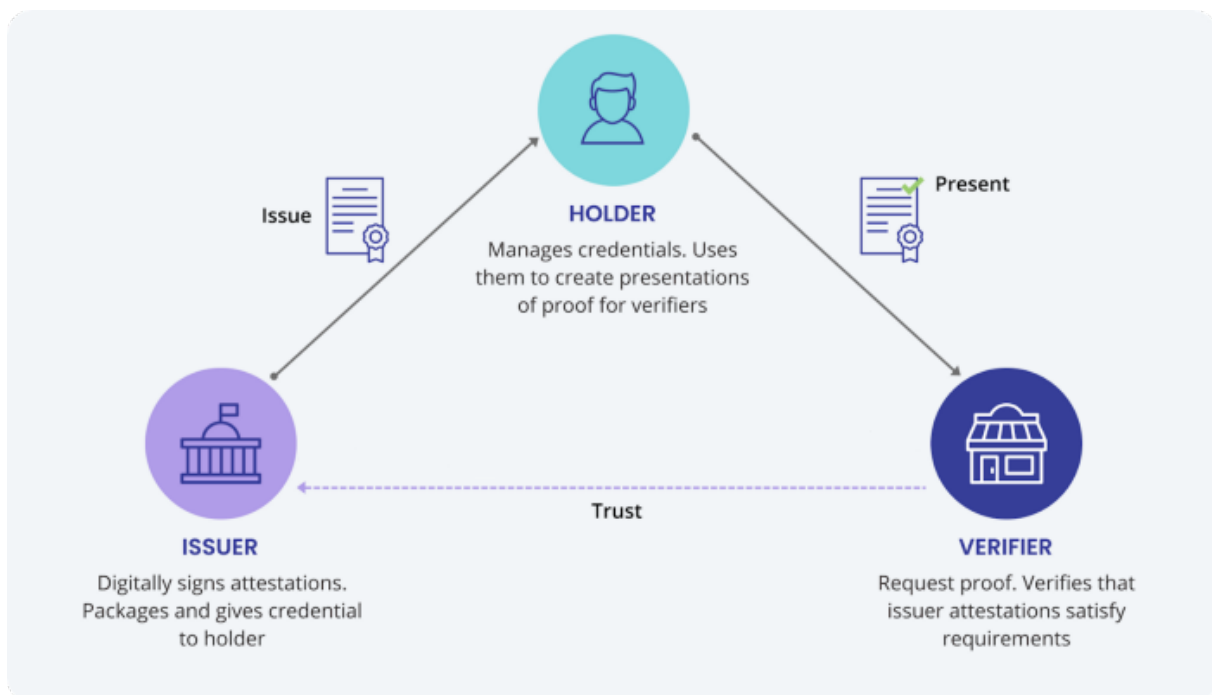
- (a) **Primary identity credentials:** are typically issued only once and represent life events, such as birth and marriage.
- (b) **Secondary identity credentials:** are issued in response to a request for authorization to demonstrate proof of affiliation or perform an action.

(c) **Tertiary identity credentials:** are issued by an authority or organization for a limited purpose.

Moreover, the SSI ecosystem is based on three important roles: issuer, holder, and verifier. As demonstrated in Figure 3.4, the issuer creates and issues credentials to the holder. Then, the holder stores and shares the received credentials with a verifier. A verifier accepts and approves the credentials that a holder presents.

## 2. SSI Standards:

Standards are an important part of the SSI ecosystem; they enable other parties to trust them. There are two fundamentally important standards that SSI uses, both developed at the W3C (Sporny et al., 2022).



**Figure 3.4.** *Self-sovereign Identity Ecosystem*

- *Decentralized Identifiers (DID):* In the past, humans have developed several networks in which they have to identify themselves or objects. For example, in postal or telephone networks, humans identify themselves with a name, addresses, or telephone numbers. Later, during the Internet era, various

identifiers have been introduced, such as IP addresses, e-mail addresses, domain names, or usernames.

In the SSI ecosystem, the decentralized identifiers (DID) are a key component to a designed SSI system, defined by the W3C (Sporny et al., 2022), and used to identify a subject (person, organization, thing, etc.) in a decentralized way. DID consists of three parts. The first one is a URL scheme identifier declared as “did”. The second is a DID method identifier that describes how a certain DID scheme can be used and resolved to DID documents. The last one is a DID method that communicates the information for the resolution.

For example: “did:dac:patient1”, “did” is URL scheme, “dac” is DID method and “patient1” is DID method-specific.

We can summarize The DID’s characteristics in the following points (Preukschat and Reed, 2021):

- (a) **Persistent:** DIDs do not need to update and do not have an expiration date.
- (b) **Resolvable:** DIDs are resolvable to retrieve additional metadata.
- (c) **Cryptographically Verifiable:** The owner of a DID can cryptographically prove control over it at any time using public and private key pairs being assigned to a DID.
- (d) **Decentralized:** A DID can be issued/ generated independently of a central authority.

Additionally, DIDs help to authenticate users based on their Verifiable credentials VC (diploma, certificate) issued by different companies.

- *Verifiable Credentials (VC):* VC is a standard method for digitally securely expressing credentials. They are created and signed by the issuer using his private key, and they include several key-value claims of the subject, such

as name, birth date, gender, etc. (Thomas et al., 2022). Additionally, the structure of a credential may comprise identifiers, metadata, claims, and proofs. Proofs are used to verify a credential concerning the properties of the credential. As a consequence, VC can include issuer information, expiry date, and time stamps, image representation, public Key for means of verification, revocation mechanisms, etc.

### 3.3 Related works

Many researchers have proposed different approaches to ensure security and data privacy in e-health systems. Thus, in this section, we have introduced a brief review related to the different security and privacy techniques.

#### 3.3.1 Encryption techniques

To secure patient data and preserve the privacy of health records in a healthcare cloud, Narayan et al. (2010) combined attribute-based cryptography and public-key encryption with keyword search to ensure privacy preserving EHR management system. ABE is used to facilitate access to the symmetric key which is generated by a trusted authority (TA). However, the privacy of data can be breached as the TA has control over all the encrypted data keys and can access the patient's data anytime.

Similarly, Hu et al. (2010) described the use of EHR's public key infrastructure (PKI) for privacy and security. To comply with HIPAA regulations, a hybrid public key infrastructure solution (HPKI) is proposed where the PKI is used to mutually authenticate and distribute health data and symmetric encryption is used to maintain the confidentiality of health data. However, in their scheme, the security management is delegated to the medical provider.

In the same context, Babrahem and Monowar (2021) proposed a cloud-based EHR system that combines the OrBAC model with the AES encryption scheme. In this

system, AES encryption is performed twice to protect the EHR data, referred to as primary and temporary encryption, with two layers of security and confidentiality.

### 3.3.2 Access control techniques

For fine-grained access control of healthcare data in cloud systems, Li et al. (2010) adopted the concept of MA-ABE (Multi-Authority Attribute-Based Encryption). However, the proposed system is unable to maintain patient data privacy in the event of a medical emergency.

Similarly, to obtain a single model limiting the user's access to medical records, Gajanayake et al. (2014) combined four access control models: DAC, MAC, RBAC, and PBAC (Purpose Based Access Control). However, this system is used only by the doctor and the patient and did not address different classes of healthcare providers. Also, the data and requests are transmitted between the client and server.

In addition, a secure system is proposed by Yang et al. (2019) to devise a novel access control mechanism, which is adaptive for both normal and emergency cases. In a normal situation, the healthcare staff can have the data access privilege with proper attribute secret keys. In an emergency, historical medical data of patients can be recovered using a break-glass access mechanism based on a password.

Also, a novel access-control system was designed by Rezaeibagha and Mu (2016) to solve the concerns about security and privacy in EHR. To ensure reliable access control and authorization-preserving data sharing among various healthcare providers, the framework used hybrid clouds as well as access control policy transformation. Some cryptographic building blocks were added with access control policy transformation to tackle different EHR users with varying access privileges and permission in various cloud settings.



### 3.3.3 Differential Privacy

Differential privacy is a rigorous mathematical definition of privacy. Consequently, Liu et al. (2019a) proposed to apply the concept of differential privacy to analyze the privacy of the eye tracking data. They have analyzed the privacy guarantees provided by random selection mechanisms, and additive noise (Gaussian and Laplacian noise).

Also, a differential protection scheme for big data is developed in the body sensor network by Lin et al. (2016). This scheme provides greater availability and reliability for privacy protection. The authors introduce the concept of dynamic noise thresholds to demonstrate the relationship between the added noise and data set size, making their scheme more suitable for big data processing. According to Zia et al. (2020), privacy is a major concern when the data is shared for further analysis or research purposes. To avoid any privacy breach, the authors discuss the differential privacy approach by using the unique property of differential privacy and applying it to healthcare data. Also, they discuss the impact of the amount of noise introduced in the original data, the relation between the added noise in the data, data utility, and the effect of data leakage on breach of privacy.

### 3.3.4 Anonymization/Pseudonymization techniques

Mohandas (2014) presented a system that integrates anonymization with the CP-ABE scheme to provide data sharing and fine-grained privacy-preserved access control. However, this approach does not address user revocation and medical emergencies are not taken into consideration.

Taneja et al. (2015) presented a model to solve the challenge of re-identification risk. Their solution is based on k-anonymity combined with l-diversity, t-closeness, and -presence, and is implemented through the ARX anonymization tool. However, much information loss was noticed.

Also, Al-Zubaidie et al. (2019) proposed anonymization and pseudonymization with the XACML modular system to solve privacy issues related to specific users. The presented system uses: (i) a random pseudonym to separate personal information about patient data, (ii) anonymity to hide the information subjects, (iii) XACML to create distributed access which can reduce unnecessary time consumption. However, authentication and security mechanisms are required for data collection and storage on the server.

### 3.3.5 Homomorphic encryption techniques

Kocabas and Soyata (2020) presented a working implementation of a long-term cardiac health monitoring application using Fully Homomorphic Encryption (FHE) as an encryption approach. FHE enables computations on private health information without actually observing the underlying data.

Similarly, Thilakanathan et al. (2014) proposed a platform for the secure exchange of patient medical data in cloud-health systems. The proposed security mechanism used a proxy re-encryption technique based on the El-Gamal approach and ensures a revocation scheme. However, it does not provide much support for complex access policies.

In the same context, Zhang et al. (2014) used Paillier Cryptosystem in their proposed framework that preserves identity and data privacy during data transmission in cloud healthcare. The framework is known as PHDA (Priority-based Healthcare Data Aggregation methodology). However; this solution has key management issues.

### 3.3.6 Blockchain techniques

To provide secure management and analysis of healthcare big data, Dwivedi et al. (2019) introduced a novel hybrid approach that combines the advantages of the

blockchain and many cryptographic primitives to develop a patient-centric access control for electronic medical records (EMR).

Similarly, Al Omar et al. (2019) presented a patient-centric healthcare data management system using blockchain technology as storage which helps to achieve privacy. Also, cryptographic algorithms are used to encrypt patient data and ensure pseudonymity. They analyze the cost-effectiveness of smart contracts and the data processing methods used in their system. However, their works do not explore the interoperability between different entities (e.g., hospital, doctors, and patients) of the healthcare process.

In the same domain, Xia et al. (2017b) presented MeDShare, a solution that focuses on the problem of medical data sharing in a secure environment. The framework is based on blockchain and provides auditing and control for shared medical data in cloud repositories. It used smart contracts and an access control model to effectively monitor data behavior.

Also, Dagher et al. (2018) presented the Ancile solution based on blockchain for efficient, interoperable, and secure access to health data by patients, providers, and third parties to preserve the privacy of sensitive information of patients. Ancile is based on Ethereum blockchain smart contracts to enhance data access control and provides advanced cryptographic techniques.

### **3.3.7 Self-Sovereign Identity Technology**

Self-sovereign identity system (SSI) helps to prove who we are to establish trusted relationships and access information. For this reason, Belchior et al. (2020) proposed the SSIBAC framework, a Self-Sovereign Identity Based Access Control system. SSIBAC is an access control system for managing identities across organizations. It offers decentralized authentication and centralized authorization using traditional access control architecture with blockchain technology.

Similarly, Lagutin et al. (2019) presented an OAuth-based method for delegating the access policy management to the authorization server, allowing systems with limited IoT devices to benefit from Decentralized ID (DID) and Verifiable Credentials (VCs). However, a complete threat analysis must be performed before using DIDs to determine whether DIDs are the right approach for the IoMT devices.

Jung (2021) proposed a decentralized access control system based on DID and explained how the proposed approach grants access privileges without a centralized authority. However, this may not be an ideal proposition against hacking like other centralized systems.

Kim et al. (2021) presented a DID-based ABAC to address the issue of ABAC's privacy exposure and implement it on a power transaction platform.

### **3.4 Summary**

The security and privacy techniques in the medical domain has been reviewed in this chapter. In the next chapters, we introduce our two contributions, which address the security and privacy issues in the e-health based F2C-IoMT system.

## **Part II**

# **CONTRIBUTIONS**

Chapter

**4**

---

# A secure health monitoring system based on Fog to Cloud computing

## Contents

---

|            |                                      |           |
|------------|--------------------------------------|-----------|
| <b>4.1</b> | <b>Introduction</b>                  | <b>74</b> |
| 4.1.1      | Motivation                           | 74        |
| <b>4.2</b> | <b>F2C architecture</b>              | <b>75</b> |
| <b>4.3</b> | <b>System model and design goals</b> | <b>76</b> |
| 4.3.1      | System model                         | 76        |
| 4.3.2      | Design Goals                         | 78        |
| <b>4.4</b> | <b>Security Model</b>                | <b>79</b> |
| 4.4.1      | Lightweight Security Scheme (L2S)    | 79        |
| 4.4.2      | Case study: fall detection algorithm | 85        |
| <b>4.5</b> | <b>Security Analysis</b>             | <b>86</b> |
| 4.5.1      | Security and Confidentiality         | 86        |
| 4.5.2      | Privacy                              | 86        |
| <b>4.6</b> | <b>Performance evaluation</b>        | <b>86</b> |
| 4.6.1      | Simulation setup                     | 87        |
| 4.6.2      | Results and discussion               | 88        |
| <b>4.7</b> | <b>Summary</b>                       | <b>91</b> |

## 4.1 Introduction

This chapter presents our first contribution for security and privacy-preserving medical data. A secure health monitoring system based on fog-to-cloud computing was proposed. It exploits the advantages of fog and cloud computing to enhance security and preserve the privacy of medical data. The main benefits of this framework are high computing and storage capabilities, reduced network traffic, and low latencies (Allen, 2016). However, using fog to cloud (F2C) computing raises many security concerns. To address these issues, it is necessary to adopt cryptography techniques to ensure the security of medical data. Therefore, the objectives of this chapter are:

1. Proposing a remote health monitoring (REM) framework based on F2C computing.
2. All medical records including personal and electronic health records must be encrypted before sharing and storing.
3. Using an hybrid encryption scheme to secure data.
4. Evaluating the proposed system by comparing the performances of fog and cloud computing.

### 4.1.1 Motivation

Nowadays, elderly people need to visit doctors regularly for their checkups and diagnosis. With the advances in technology, the emergence of the internet of medical things (IoMT) will facilitate the development of elderly remote monitoring systems (Ahmid et al., 2022), (Silas and Rajsingh, 2019). Additionally, the deployment of computing models throughout hospitals is crucial to share health data with different users (Saidi et al., 2020). These technologies allow elderly persons to be assisted by health professionals in their home, enable physicians to follow their diseases, and

provide suggestions in real-time (Almeida et al., 2017). Also, to collect real-time medical data, wearable sensors can be used. These sensors will generate huge amounts of data that must be processed rapidly and stored sustainably by using innovative storage infrastructures. Therefore, F2C computing plays an extremely important role in these circumstances to process and store medical data. However, using F2C computing raises many security concerns (leakage, waste, or theft). To overcome these challenges, it is necessary to reinforce security measures by adopting cryptography techniques. Indeed, privacy and security issues must meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

## 4.2 F2C architecture

The first attempt to implement the F2C architecture has been done in the framework of the European H2020 mF2C project (Salis, 2022). As illustrated in Figure 4.1, the F2C architecture is distributed and it has a hierarchical layered design, it can offer high performance, more energy efficiency, real-time processing, scalability, and close localization for IoT and edge devices. Also, it enables a multi-layer resource allocation as well as the distributed and parallel service execution in fog resources, cloud, or both. Therefore, the F2C model can increase the number of layers on a large scale with millions of IoT devices to facilitate efficient coordination between nearby areas and provide scalability features.

To set the F2C architecture, the layers must be defined, grouping a set of resources and enabling services to decide the set of resources, be at the fog, cloud, or both of them. Fog devices may be some other common devices, such as small servers, routers, access points, or gateway. Moreover, the management of resources becomes a key challenge to efficiently manage resources and optimize service execution. Additionally, one fog node must be selected as a manager of the fog layer for handling other fog devices and IoMT devices, managing the devices inside the fog, and collaborating with higher-level layers.



However, the cloud's resources are implemented in the form of several virtual machines (VMs), each of which can be configured to a particular configuration, whereas the devices in the fog layer have constrained processing capabilities. Therefore, it is apparent to try to accomplish the task using cloud resources if the available resources are insufficient or unavailable at all in the fog.

In general, the functionality of a fog device can be described as follows. The fog device processes and stores all medical data once received. Then, data will be sent to the cloud, which is responsible for the long-term storage of processed data and application outcomes.

### 4.3 System model and design goals

In our framework, older persons are monitored in real-time permitting different users (doctors, nurses, pharmacists, researchers, etc.) to access health data at any time and from anywhere.

#### 4.3.1 System model

The architecture of our system is composed of the following layers: the IoMT devices layer, the gateway layer, the end-user layer, and the F2C computing layer, as presented in Figure 4.1.

- **IoMT devices layer:** includes several types of wearable sensors such as blood pressure sensors, body temperature sensors, etc. The IoMT devices are allowed to initiate the process by sensing and collecting medical data. Data sensed are compared with the previous data value, only the difference data is transmitted to the gateway to minimize the number of packets circulating in the network and save sensors and mobile energy.

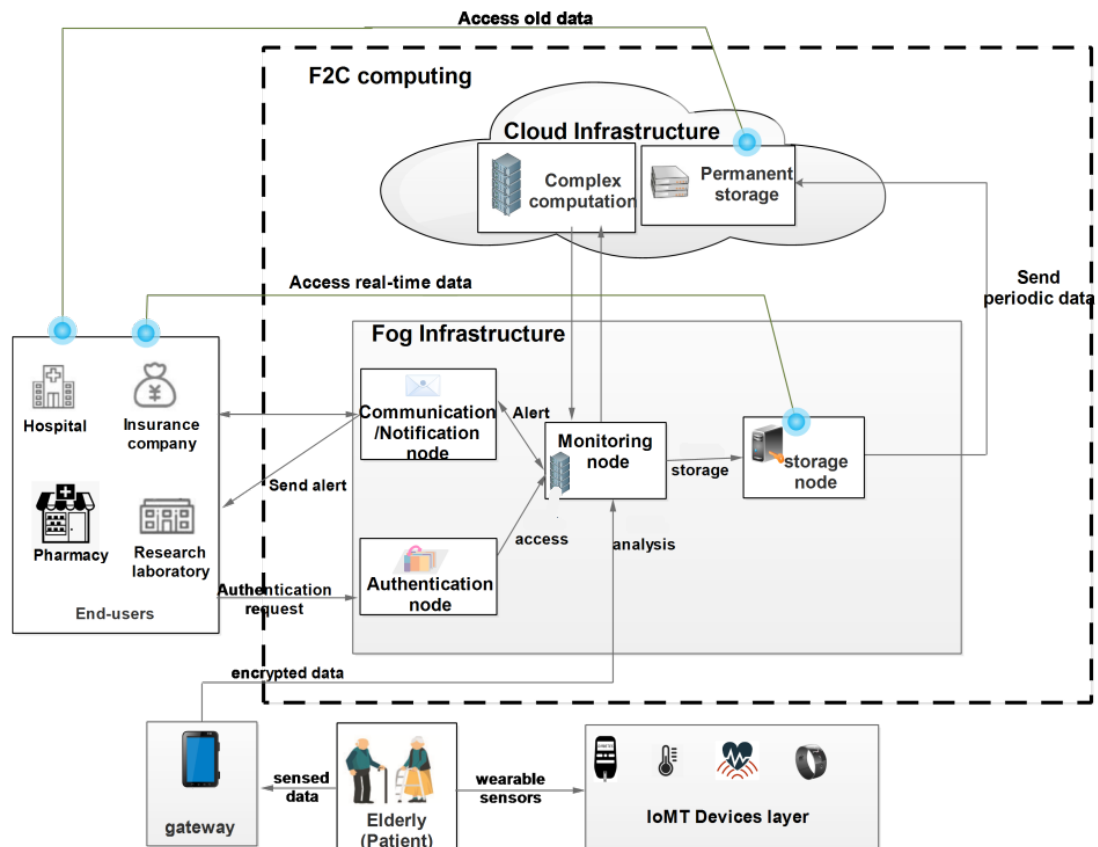


Figure 4.1. System overview

- **End-user layer:** This layer includes all remote users who assist the elderly such as physicians, nurses, pharmacists, and family members. The end-user has different privileges under diverse situations.
- **Gateway layer:** plays a key role in our model by bridging the gap between the IoMT devices layer and the F2C computing layer. It is based on the mobile phone and is used to pre-process the sensed data by performing the health records' encryptions. The resulting ciphertext is transmitted to the F2C computing layer.
- **F2C computing layer:** consists of two sub-layers:

1. **Fog computing:**

It is used to perform filtering, storing, analyzing, and processing of encrypted medical data in real-time. However, it has limited storage and computing resources compared to the cloud. It uses simple, less complex algorithms for data acquisition and analytics. Since it continuously monitors

the sensor nodes, it can be used to generate notifications to avert incidents.

In our study, fog computing is composed of the following nodes:

- *Authentication node* - the authentication phase is crucial in the healthcare domain, it plays a significant role in remote elderly monitoring (REM) systems to protect patients' privacy and security.
- *Temporary storage node* - This node provides transient storage of the encrypted data and sends periodic data to the cloud for permanent storage.
- *Monitoring node* - This node aims to analyze data, prevent and detect elderly diseases, and provide useful information about the elderly. In addition, it manages notifications if an emergency occurs.
- *Communication and notification node* - Through this node, all end-users can collaborate securely, and work together to improve the elderly's health.

## 2. Cloud computing:

This sub-layer is located in the top layer of the F2C, it securely stores medical data sent by the fog and generates historical analysis reports. However, for real-time analysis and emergency notifications, the fog computing platform is the optimal solution.

### 4.3.2 Design Goals

Our design goals concentrate on presenting an efficient, secure, and privacy-preserving medical data scheme, according to the system model.

1. *Efficiency.* the proposed system should support the real-time transmission of health records from a vast number of IoMT devices.
2. *Security.* the proposed scheme should enable strong confidentiality of data transmission.

3. *Privacy Preservation.* An attacker should not have access to patients' personal data during system communications. Even if several IoMT devices cooperate, they should not infer other patients' private data.

## 4.4 Security Model

Sensing and transmitting data to the gateway are the primary responsibilities of IoMT devices. However, security and privacy are crucial considerations.

Generally, data security is maintained by encrypting the sensed data using one or several kinds of encryption algorithms, such as asymmetric and symmetric key algorithms. The data encryption algorithms based on asymmetric keys like RSA and ECC (Jung, 2021) achieve a high level of security. However, they are not preferable for IoMT devices which have limited resources, in terms of processing power, memory, and storage. On the other hand, data encryption algorithms based on symmetric keys like DES and AES (Abdullah et al., 2017) don't require huge computational power and storage, but a key exchange scheme is still required.

### 4.4.1 Lightweight Security Scheme (L2S)

To solve challenges related to symmetric and asymmetric algorithms and prevent unauthorized access and data modification, we propose a Lightweight Security Scheme (L2S). L2S is a hybrid algorithm that incorporates the advantages of two encryption schemes, the Advanced Encryption Standard (AES) (Abdullah et al., 2017), and Elliptic Curve Cryptography (ECC) (Jung, 2021), in terms of encryption and decryption time, security, key management, and key size (Sood, 2012).

The L2S algorithm is considered as lightweight scheme because the key generation time was calculated as the lowest in comparison with other encryption algorithms (Habib et al., 2018) with the smallest key size, while maintaining the security of the system. The next section explains the encryption and decryption steps of L2S scheme.

#### 4.4.1.1 Problem Statement

Different encryption algorithms can be deployed to secure the transmission of medical data. However, the major issue with these algorithms is that they need a large memory size and a large key size, and require a lot of computation power. For instance, AES uses a symmetric key encryption method in which a single key is used for encryption as well as decryption. Whereas, if the single key is known by the third party, then the data will easily be decrypted and again encrypted so that the user does not know that the data has been read by someone else. Also, ECC uses asymmetric keys encryption in which two keys for encryption and decryption are generated, public and private key, respectively. The main benefit of ECC algorithm is its smaller keys size, so it provides a higher level of security, making it difficult for hackers to crack both keys. However, ECC encryption significantly increases the size of the encrypted message compared to RSA encryption. It is more difficult and complex to implement than the RSA algorithm, which increases the possibility of implementation errors. Thus, there is a need to propose an algorithm that provides a higher level of security with less computational cost, smaller key size, and less time for the encryption and decryption processes.

In summary, we combine the properties of both algorithms and utilize them in our proposed security protocol.

#### 4.4.1.2 ECC and AES algorithms

##### 1. ECC algorithm

ECC is considered the ideal modernized successor for the RSA cryptosystem. It requires smaller keys and signatures than RSA to achieve the same level of security, and offers fast key generation. It focuses on pairs of private and public keys based on the algebraic structure of elliptic curves over finite fields. Instead of the traditional methods used to create keys, ECC produces keys using the properties of the elliptic curve equation. An elliptic curve is a set of points that

satisfy a specific mathematical equation. The equation has the form:

$$y^2 = x^3 + ax + b \quad (4.1)$$

in which  $a$  and  $b$  are consistent (Sood, 2012).

The advantages of the ECC cryptosystem are (i) small key size, (ii) less computational time, (iii) higher key generation and exchange rate, and (iv) lower computing power and battery resource usage. For these reasons, ECC is becoming widely used for mobile applications (Bhardwaj and Chaudhary, 2012). However, the main disadvantage of ECC is that it is not easy to implement it as the RSA algorithm, which increases the possibility of errors.

- *Key generation*

To generate the public and private keys, we assume that we have two users  $A$  and  $B$  who want to connect and share information. Both agree on a common elliptical curve equation with the coefficients  $a$  and  $b$ , a generator  $Q$  that generates cyclic subgroup and the order  $n$  of the subgroup (Kute et al., 2009).

- $A$  selects an integer  $n_A$  chosen from  $\{ 1, \dots, n-1 \}$ , where  $n$  is the order of the subgroup. The Private Key of  $A$  is:

$$A = n_A (n_A < n) \quad (4.2)$$

and the Public key  $P_A$  of  $A$  is calculated as follows:

$$P_A = n_A \times Q \quad (4.3)$$

- $B$  similarly selects an integer  $n_B$ , the Private key of  $B$  is:

$$B = n_B (n_B < n) \quad (4.4)$$

and the Public key  $P_B$  of  $B$  is calculated as follows:

$$P_B = n_B \times Q \quad (4.5)$$

- *ECC Encryption* (Kute et al., 2009)

To conduct confidential communications between sender  $A$  and receiver  $B$ . We take one plaintext block  $m$  which has been mapped into the point  $P_m(x_m, y_m)$  of elliptic curve. According to the key pair generation algorithm, the encryption process is designed as follows.

- Encode the plain text  $m$  to be sent as an  $P_m(x_m, y_m)$  point.
- Require a point  $G$  and an elliptic group  $E_P(a,b)$  as parameters.
- $A$  chooses a random positive integer  $k$ .
- $A$  then produces the ciphertext  $C_m$  based on the pair of points:

$$C_m = \{k \times G, P_m + k \times P_B\} \quad (4.6)$$

- *ECC Decryption* (Kute et al., 2009)

The encryption data received by  $B$  is two point,  $(P_1, P_3)$  with  $P_1=KG$ ,  $P_3=P_m(x_m, y_m)+P_2$  and  $P_2=KP_B$ . The decryption process for receiver  $B$  is described as follows:

- Receiver  $B$  computes:

$$P_m + k \times P_B - n_B (k \times G) = P_m + k (n_B \times G) - n_B (k \times G) = P_m \quad (4.7)$$

- $A$  has masked  $P_m$  by adding  $k P_B$  to it.

2. **AES algorithm** The Advanced Encryption Standard (AES) is a symmetric encryption type that uses only one key for encryption and decryption processes. AES is one of the types of cipher text which uses the block cipher (Sood, 2012). The size of the block is 128 bits, and the length of the key can be 128, 192, or 256 bits. The AES is based on the following modules: Encryption, Decryption, and Round Key Generator. The encryption module consists of the input block

(plain text), the intermediate values of this block (states), and the returned block (cipher text). AES encryptions and decryptions are based on different operations, called *AddRoundKey*, *SubBytes*, *ShiftRows*, and *MixColumns*. For the decryption algorithm, the operations are the inverse of the encryption operations, *AddRoundKey*, *InvShiftRows*, *InvSubBytes*, and *InvMixColumns* (Mendonca, 2018). *AddRoundKey* was realized in the first Round. Rounds consist of *SubBytes*, *ShiftRows*, and *AddRoundKey*, as described in the following steps (Shao et al., 2010):

- *SubBytes*: a non-linear substitution step that replaces each byte with another based on a lookup table.
- *ShiftRows*: a transposition step where each row of the state is shifted cyclically over a certain number of steps.
- *MixColumns*: mixing operations that are applied on the columns of the state, combining the four bytes in each column
- *AddRoundKey*: each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

These operations are applied to a 128-bit input block in a certain sequence to perform an AES encryption or decryption. In both cases, the operations are grouped into rounds, the number of these rounds,  $N_r$ , depends on the key size.

#### 4.4.1.3 Combined hybrid algorithm AES-ECC (L2S)

ECC is the most appropriate technique to use along with AES to get the data secured from unauthorized use (Hafsa et al., 2017). The combination of ECC and AES (L2S) creates the most advanced and efficient cryptographic techniques. The L2S allows reduced key size as well as a faster security mechanism for securing the data (Mendonca, 2018). As shown in Figure 4.2, the AES algorithm is used to encrypt and decrypt medical data while the ECC technique is used to encrypt and decrypt the AES key.



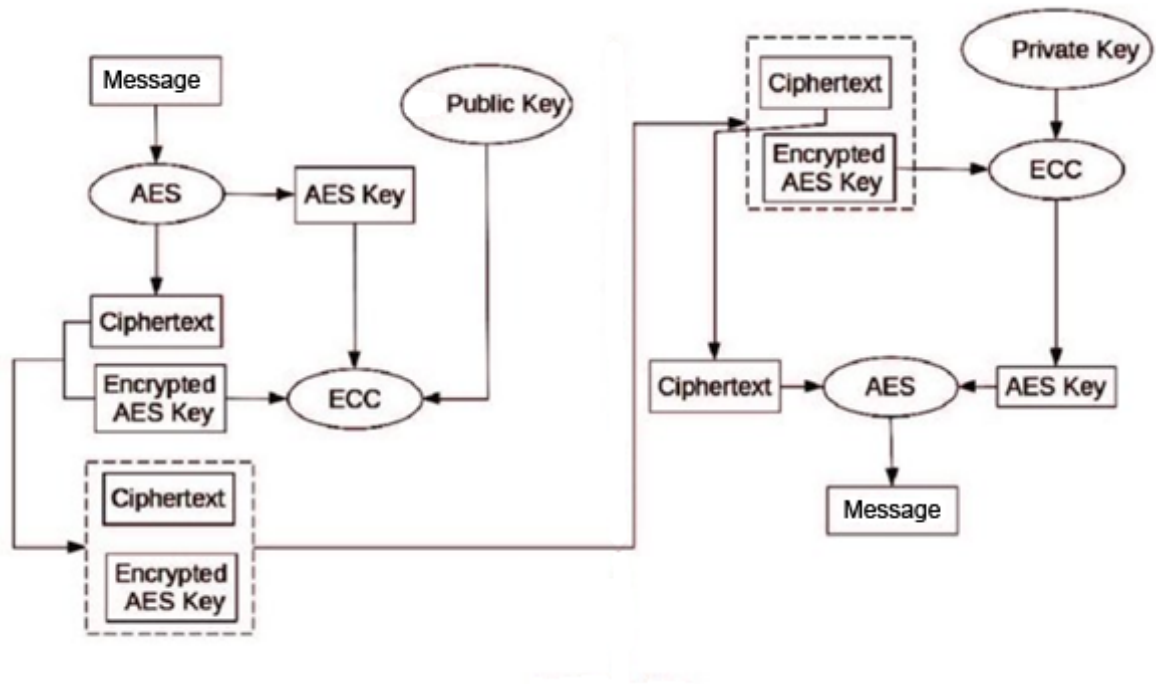


Figure 4.2. Flow chart of L2S

Therefore, the L2S consists of three stages which are: the key generation stage, encryption stage, and decryption stage.

1. ECC keys generation

- Choose a prime number  $n$ .
- Choose a number  $P$  for the generation of the public key, where  $P < n$ .
- Determine the point on the curve as  $G$ , where  $G > n$ .
- The public key is calculated as follows:

$$PK = P \times G \tag{4.8}$$

2. Encryption phase

- An AES key  $k$  is chosen.
- Encrypt data  $D$  using AES key  $k$ .
- Then, AES key  $k$  is encrypted using the ECC algorithm, generates  $(k_e)$ , and adds it to the ciphertext  $(D_e)$ .

- The encrypted data ( $D_e$ ) and AES encrypted key ( $k_e$ ) are transmitted to the fog storage.

### 3. *Decryption phase*

- The encrypted AES key ( $k_e$ ) is decrypted with the ECC algorithm.
- Then, the encrypted data ( $D_e$ ) is decrypted by the AES algorithm using key  $k$ .

## 4.4.2 Case study: fall detection algorithm

To illustrate the different features of our system, we describe a case study in which medical data of the elderly are managed through our framework. Fall in the elderly population is one of the most important monitoring cases that we can study. When a fall has happened, the IoMT devices layer collects and sends the acceleration data to the gateway (mobile phone) (Saidi et al., 2019). The gateway will generate an AES symmetric key and encrypt all the personal and medical data. The AES symmetric key will then be encrypted using the ECC public key of the patient. The encrypted data and encrypted symmetric key will then be sent to fog computing.

To share the data with a geriatrician, the gateway will divide the patient's ECC private key into two parts. The first partition will be sent to the fog storage and the second one will be sent to the geriatrician. By doing this, the untrusted user does not know the full private key. When the geriatrician receives the notification, he sends an access request to the authentication node. If the request is accepted, the fog partially decrypts the AES symmetric key using the partial key supplied by the gateway and sends the encrypted data contents and partially decrypted symmetric key to the geriatrician. The doctor uses the ECC partial key received from the gateway to fully decrypt the symmetric key and finally decrypt the data contents. Thus, the geriatrician can check the fall parameters such as the elderly location, and then he uses the communication node to call an ambulance.

## **4.5 Security Analysis**

The main aim of the proposal is to ensure the security and privacy of the medical data stored in the F2C storage.

### **4.5.1 Security and Confidentiality**

L2S hybrid algorithm enables strong confidentiality of the medical data. We adopt two encryption levels to guarantee the confidentiality of medical data, since a good encryption scheme should resist all kinds of known attacks. In our proposed approach, the data is fully encrypted with the help of AES-ECC algorithms. Therefore, if an attacker gets access to the data, it will be useless because the information was already encrypted and the attacker has no knowledge of the AES-ECC keys. Thus, the hybrid algorithm protects sensitive data from unauthorized access and attacks.

### **4.5.2 Privacy**

Our scheme can protect patients' privacy through the L2S. During the communication and data transmission process, the attacker cannot learn any personal information about the patient because we also utilize AES-ECC encryption to protect personal data. This will resist any attacks from both outsiders and insiders attempting to obtain sensitive data without permission. Thus, the patient's privacy is protected with the security of health data.

## **4.6 Performance evaluation**

In this section, we discuss some simulation results showing the impact of our proposed framework-based F2C solution on facilitating the remote monitoring of elderly people without violating HIPAA compliance.

We have used the FogWorkflowSim (Liu et al., 2019b) simulator to demonstrate the impact of deploying our framework on fog computing instead of cloud computing.

### 4.6.1 Simulation setup

The fundamental basis of the simulator FogWorkflowSim is the simulation of a fog computing environment with a workflow system. It inherits the functions of iFogSim (Liu et al., 2019b) and WorkflowSim simulators, and it is developed in Java JDK 1.8. Indeed, FogWorkflowSim is a powerful tool for analyzing resources and task management techniques in fog Computing. Specifically, it can:

1. Set up a simulated F2C environment.
2. Execute workflow applications.
3. Evaluate the performance of different tasks based on the following performance metrics: time, energy, and cost.

We have installed it on a desktop computer with the following characteristics: Intel core i7-6500U, CPU 2.50 GHz, 8 GB RAM, and Microsoft Windows 10 OS.

To store the performance metrics and computation techniques, many libraries are used like All-in-Fog (without the use of cloud Servers), All-in-Cloud (without the use of fog Nodes), and Simple. These libraries include many workflow scheduling algorithms such as MinMin, MaxMin, First Come First Serve (FCFS), RoundRobin, Particle Swarm Optimization algorithm (PSO), and Genetic Algorithm (GA) (Liu et al., 2019b), as illustrated in Figure 4.3.

In our experiments, the Montage workflow has been used to evaluate the impact of a diverse number of tasks performed in cloud and fog computing based on the following performance metrics: latency, energy, and cost.

### 4.6.2 Results and discussion

In our F2C environment, we consider the infrastructure based on 1 fog computing, 1 cloud computing, and 5 IoMT devices, as shown in Figure 4.3.

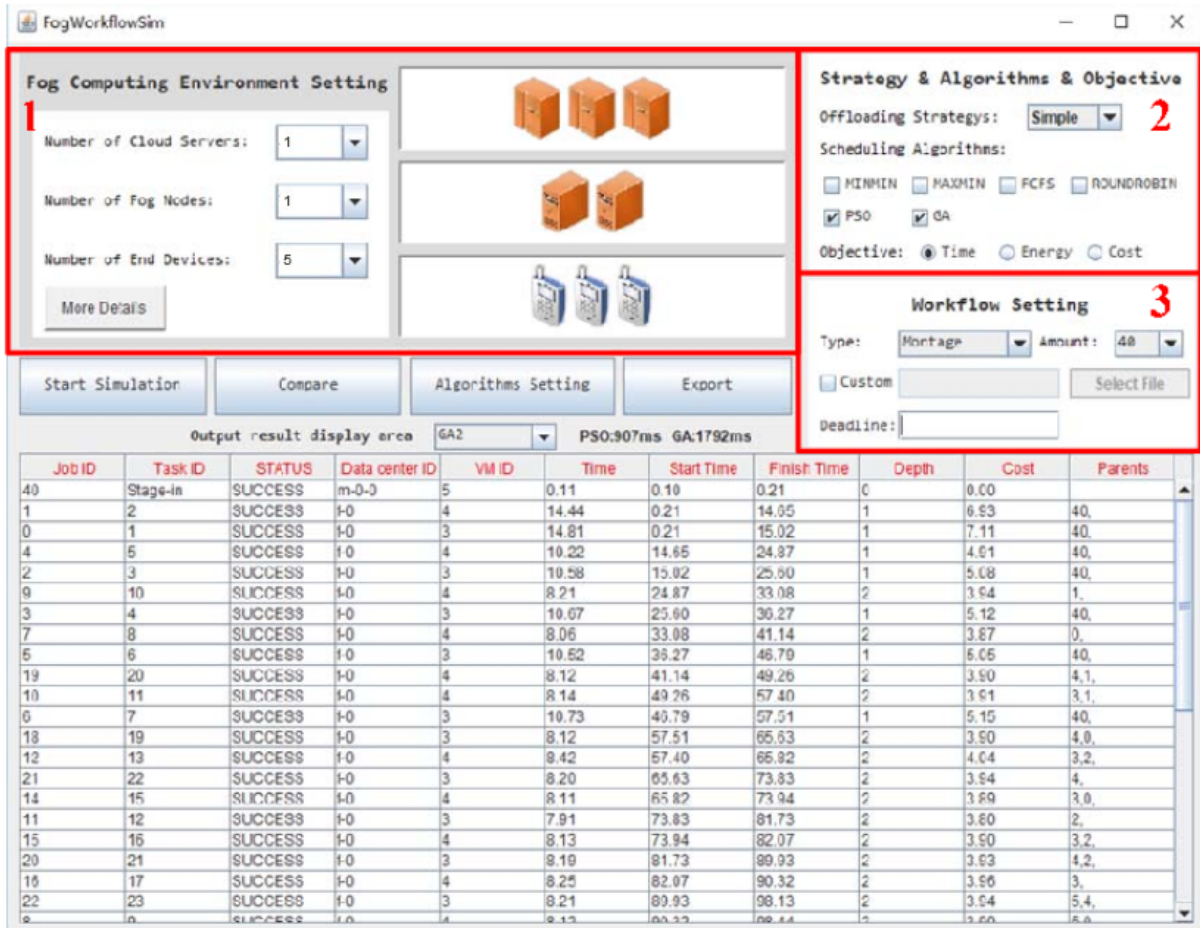


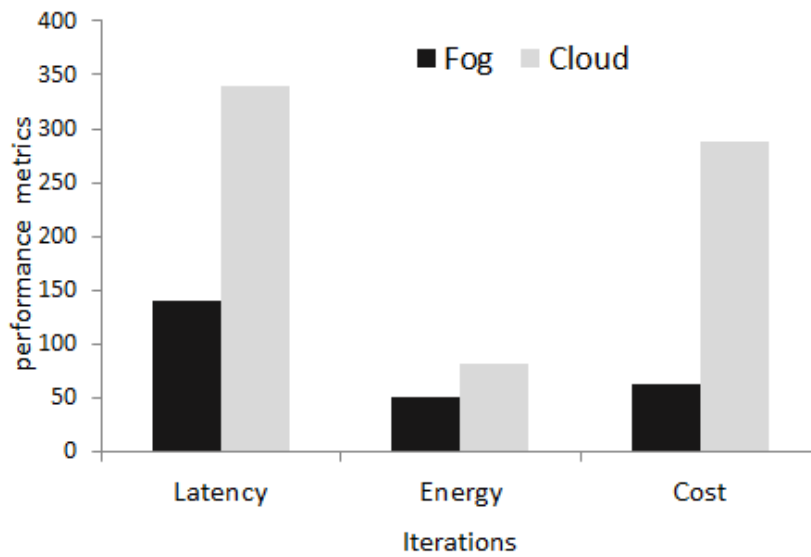
Figure 4.3. Main page of FogWorkflowSim

A summary of experimental results on latency, energy consumption, and cost consumption in both fog and cloud computing is shown in Figure 4.4. We can observe that using the fog layer reduces the latency, energy consumption, and cost when compared to using only cloud computing, as shown in Table 4.1.

We have also compared the performance evaluation of our scheme with those of the (Gill et al., 2018) scheme. The authors proposed a model that manages the data of heart patients. They have used the iFogSim toolkit to analyze the performance of the proposed model in a Fog-enabled cloud environment.

**Table 4.1.** Comparison of performance parameters of two different environments.

|                        | Average Latency (s) |                          | Average energy consumption (Joules) |                          | Average cost (\$) |
|------------------------|---------------------|--------------------------|-------------------------------------|--------------------------|-------------------|
|                        | <i>Our model</i>    | <i>Gill et al. model</i> | <i>Our model</i>                    | <i>Gill et al. model</i> | <i>Our model</i>  |
| <b>Cloud computing</b> | 0.337               | 24.33                    | 79.11                               | 101.30                   | 288               |
| <b>Fog computing</b>   | 0.138               | 8.30                     | 48.58                               | 51.10                    | 63                |



**Figure 4.4.** Summary of experimental results

We notice in Figure 4.5 that fog performs better than the cloud in terms of latency; it reduces by 41% average latency as compared to the cloud. Also, we observe that the latency computed by the simulator used in our model is less than the latency computed in the (Gill et al., 2018) model. Figure 4.6 describes the consumption of energy for fog and cloud environments to process different numbers of tasks launched by sensor patients. Fog reduces 44% of average energy consumption as compared to the cloud. From the results, we observe that the energy consumption computed by the simulator used in our model is less than the energy consumption computed in the (Gill et al., 2018) model. Figure 4.7 shows the results on task execution cost. We can note that

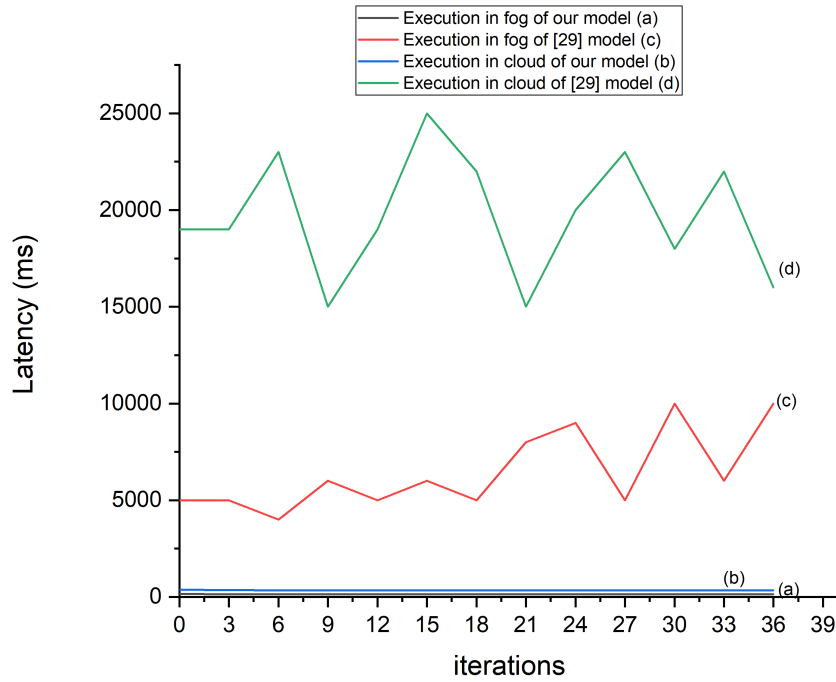


Figure 4.5. Latency comparison

the execution cost in fog computing is lower than in the cloud. This shows that fog computing is the better one for cost optimization.

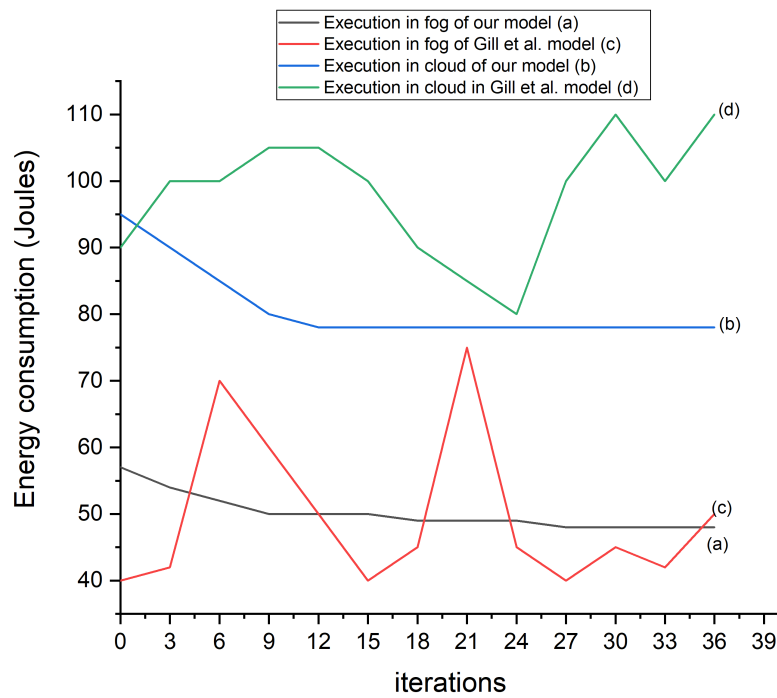
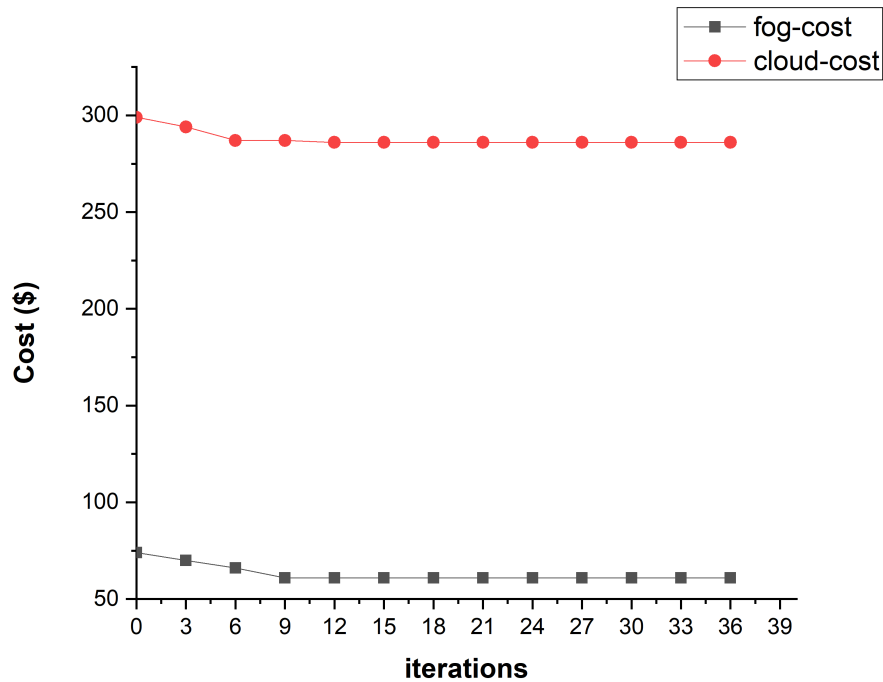


Figure 4.6. Energy consumption comparison



**Figure 4.7.** Execution cost comparison

From the simulation results, we notice that the proposed scheme is better than others in terms of latency, energy consumption, and cost. Furthermore, it shows the efficiency of using fog for data processing and cloud computing just for storage. These simulation results indicate the impact of our proposed F2C-based solution aiming to better and faster make decisions regarding the illness of elderly people.

## 4.7 Summary

This chapter proposes a framework for elderly health monitoring systems based on F2C computing that ensures high computing and low latencies, as well as enhances the security and privacy of personal and electronic health data as recommended by HIPAA. In addition, this chapter aims to set up approaches to boost the security of medical data and the privacy of personal data in the F2C environment. For this reason, a lightweight algorithm (L2S) was proposed based on the AES-ECC hybrid protocol.



The performance of our model is evaluated using the FogWorkflowSim toolkit, which demonstrates that fog computing increases the efficiency of the entire system. We noticed that the proposed scheme is better than others in terms of latency, energy consumption, and cost. Furthermore, it shows the efficiency of using fog for data processing and cloud computing just for storage. These simulation results indicate the impact of our proposed F2C-based solution aiming to better and faster make decisions regarding the illness of elderly people.

Chapter

**5**

---

# A novel decentralized framework for privacy-preserving and securing medical data sharing

## Contents

---

|            |   |            |
|------------|---|------------|
| <b>5.1</b> | <b>Introduction</b>                                 | <b>94</b>  |
| 5.1.1      | Motivation  | 95         |
| <b>5.2</b> | <b>Background knowledge</b>                         | <b>96</b>  |
| 5.2.1      | Self-Sovereign Identity (SSI)                       | 96         |
| 5.2.2      | Blockchain  | 102        |
| 5.2.3      | Access control                                      | 105        |
| 5.2.4      | Zero-Knowledge Proof (ZKP)                          | 109        |
| <b>5.3</b> | <b>Models and security requirements</b>             | <b>109</b> |
| 5.3.1      | System model  | 110        |
| 5.3.2      | Adversary model                                     | 112        |
| 5.3.3      | Security requirements and design goal               | 114        |
| <b>5.4</b> | <b>Proposed DSMAC scheme</b>                        | <b>115</b> |
| 5.4.1      | Towards a decentralized access control scheme       | 115        |
| 5.4.2      | Decentralized Access Control Scheme Based-SSI model | 118        |

|            |  |            |
|------------|--|------------|
| 5.4.3      | Decentralized Access Control scheme using Blockchain-based SSI model . . . . . | 121        |
| <b>5.5</b> | <b>Experiments and Results . . . . .</b>                                       | <b>126</b> |
| 5.5.1      | Experimental setup . . . . .   | 126        |
| 5.5.2      | Experimental Analysis . . . . .  | 132        |
| <b>5.6</b> | <b>Security and privacy analysis . . . . .</b>                                 | <b>137</b> |
| 5.6.1      | Comparison of security properties . . . . .                                    | 137        |
| 5.6.2      | Privacy protection . . . . .   | 139        |
| 5.6.3      | Access Control protection . . . . .  | 139        |
| 5.6.4      | Attacks analysis . . . . .   | 140        |
| <b>5.7</b> | <b>Summary . . . . .</b>   | <b>142</b> |

---

## 5.1 Introduction

This chapter proposes the DSMAC framework, a Decentralized Self-Management of data Access Control system based on blockchain (Kumar and Tripathi, 2021) and Self-Sovereign Identity (SSI) (Kondova and Erbguth, 2020) technologies. One of the strongest points of DSMAC is providing a high level of privacy as well as giving patients mechanisms to maintain control over their personal data and enabling them to manage access privileges to their medical data.

Experimental results based on privacy-preserving medical records demonstrate the effectiveness of the DSMAC scheme which is distinct from the works discussed in the literature by integrating a hybrid level of the decentralized access control model. Therefore, it considers both the “role” concept (Cruz et al., 2018) and the “attributes” (Song et al., 2020) as important topics. Later on, a comparative table is drawn to summarize the characteristics of different schemes based on privacy-preserving medical records including DSMAC.

The remainder of this paper is organized as follows: In Section 2, we provide background knowledge. We formally define the models and security requirements in Section 3, followed by our proposed decentralized access control scheme in Section 4. We report and discuss evaluation results in Section 5. Security and privacy analysis are described in Section 6. Finally, we conclude the paper by a conclusion.

### **5.1.1 Motivation**

Over the past few decades, the world has become more connected with the wide adoption of wireless communication technologies and mobile devices. This evolution lets healthcare organizations and researchers think about benefiting from these technologies to solve the current challenges (Ari et al., 2020). Accordingly, patients are increasingly exploiting mobile devices for their medical needs to promote the availability of their medical data and to help avoid repeated examinations. However, the sharing and privacy of medical data represent major technological, legal, and operational challenges.

Likewise, the identification of the patient is of critical importance for performing transactions with different healthcare organizations (Lippi and others J, 2017). However, patients find themselves having to maintain or memorize many combinations of accounts, and they may get privacy and identity loss issues. To improve the patient's identity model, we are considering the concept of Self-Sovereign Identity (SSI) (Kondova and Erbguth, 2020). In addition, the deployment of an access control model took part in our work because the patient's medical data are accessible to individuals who have diverse privileges under different situations. Therefore, the aforementioned issues will need a suggestion of a new access control model based on SSI technology. Also, proposing a blockchain in that situation can be more beneficial for the healthcare requirements in terms of immutability, decentralization, traceability, transparency, and data security and privacy (Xu et al., 2019). Notably, we take into consideration emergency cases in which the patient is unable to grant access to doctors.

## 5.2 Background knowledge

In this section, the background of our proposed system is discussed. First, we present the Self-sovereign identity (SSI) ecosystem. Then, we present different components of blockchain technology and access control models. Finally, we provide background knowledge about the ZKP protocol.

### 5.2.1 Self-Sovereign Identity (SSI)

More than 1.1 billion people in the world can not access vital services including healthcare, social protection, education, and finance because they are unable to prove their identity (Beduschi, 2019). Thus, digital identities could significantly help to address this issue and provide people with the opportunity to join society's services. These issues gave rise to the concept of a Self-Sovereign Identity system which gives users complete control over their identity data, i.e. they can decide what, to whom and how much data is shared without being dependent on a central authority.

#### 5.2.1.1 Identity

To identify a human being, various attributes can be used such as the name, gender, place of residence, profession, hobbies, religion, or even a combination of all these attributes. Therefore, digital identities are a collection of information about a person. They allow entities to authenticate themselves safely and securely through certain attributes and thus prove their identity.

#### 5.2.1.2 Digital Identity stages

Since the existence of the Internet, digital identities have evolved through four major stages.

1. *Centralized Identity*: An Identity that is granted and validated by a single hierarchy or party is known as a centralized identity. So, the user must manage several login credentials, and the services must store a lot of sensitive data safely based on data protection rules. However, they have full control over the data.
2. *Federated Identity*: The goal of federated identities is to enhance the centralized identity issues based on a single authority. Thus, in this stage, identity control was to be divided between federated authorities. It enables authorized users to access multiple domains and applications using a single set of credentials. Also, it links an individual's identity to several identity management systems so they can access securely various applications.
3. *User-Centric Identity*: The user-centric identity aims to enable individuals to maintain control over their identities across multiple authorities. Thus, the right of individuals to manage their own digital identities was one of their major objectives. They also have the choice of what data is collected and who gets access to which parts.
4. *Self-Sovereign Identity*: The most recent stage of digital identity, known as Self-Sovereign Identity (SSI), aims to address the problems of all other stages. Allen (2016) stated the ten principle keys of the Self-Sovereign Identity as follows:
  - *Existence*: In the SSI system, it must exist an independent individual.
  - *Control*: The person must have full control of his identity.
  - *Access*: The person must have continuous access to his data.
  - *Transparency*: Used algorithms should be free and open-source.
  - *Persistence*: The data must be kept as long as the user desires.
  - *Portability*: The data should be transportable and the system should not be restricted to a singular third party.
  - *Interoperability*: Data should be available as widely as possible.
  - *Consent*: The individuals must have consent for the use of their data.
  - *Minimization*: Claims' disclosure must be minimized.

- *Protection*: The system must always protect user identity.

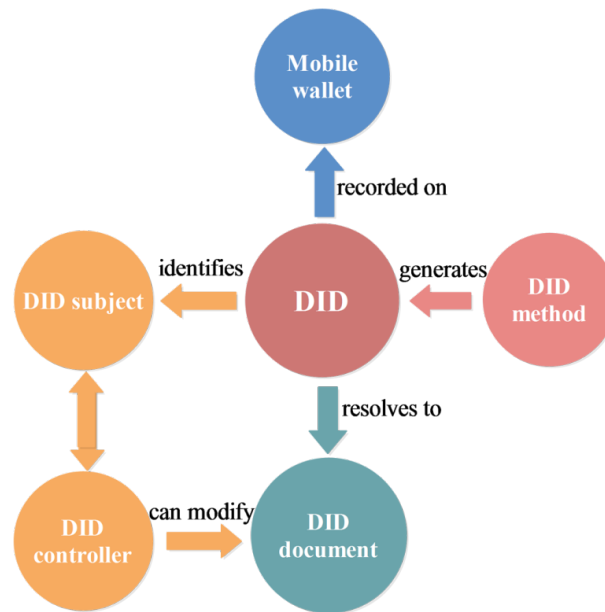
### 5.2.1.3 SSI Standards

SSI is a novel and decentralized model for digital identity. Its goal is to give individuals the authority to own and manage digital credentials (Lim et al., 2022). Therefore, it helps to prove who we are, based on the following standards: Verifiable Credential (VC) and Decentralized Identifier (DID) (Thomas et al., 2022). Both DID and VC are the twin pillars of the SSI system. In this section, the two standards are discussed in more detail.

1. *Decentralized Identifier (DID)*: DIDs represent a string identifier of a subject (person, organization, thing, etc.) and are defined by the W3C (Sporny et al., 2022). They are characterized by the following features (Sporny et al., 2022):
  - (a) *Persistent*: DIDs have no expiration date and do not require changes.
  - (b) *Resolvable*: DIDs are resolvable to get more metadata.
  - (c) *Cryptographically Verifiable*: A DID's owner is always able to use cryptography to demonstrate their ownership of the DID. This is enabled by a public and private key pair that is assigned to a DID.
  - (d) *Decentralized*: A DID can be generated and issued without the assistance of a central authority.

Figure 5.1 presents the DID architecture with all of its elements and relations. A DID method is a detailed description of how a DID is resolved to a DID Document and how DID Documents are created and modified.

Moreover, a DID Document is a structure that contains information about the identity, such as public keys, it includes references to service endpoints, such as a repository for VCs. Besides, DIDs are stored in a digital wallet that contains the user's DID, VCs, and the private key used to sign transactions and access requests.



**Figure 5.1.** The basic components of DID architecture



**Figure 5.2.** DID Format

Additionally, DID is composed of three parts, as shown in Figure 5.2. The first part contains “did” word, it represents a URL scheme identifier. The second part announces the DID method identifier. The last part is a DID method that communicates the information for the resolution.

- “did” = URL scheme identifier,
- “example” = DID method identifier,
- “123456789abcdefghijkl” = DID method-specific.

2. *Verifiable Credential (VC)*: A verifiable credential is a digital file containing several key-value claims of a subject like a name, birth date, gender, etc. (Thomas et al., 2022), as illustrated in Figure 5.3. VC represents a digital form of a credential that can be used online and protects the holders’ privacy, it is composed of metadata, claims, and proofs. Proofs are used to verify a credential (Thomas et al., 2022).



Therefore, the issuer creates and signs credentials using its private key, and allows a third party to verify the VC. The verifier can search for the issuer's public key associated with his DID and a specific credential on a distributed ledger (public blockchain).

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1"
  ],
  "id": "http://example.edu/credentials/42",
  "type": ["VerifiableCredential"],
  "issuer": "did:dac:12345",
  "issuanceDate": "2022-06-02T12:00:00Z",
  "expirationDate": "2022-12-02T12:00:00Z",
  "credentialSubject": {
    "id": "did:dac:67890",
    "name": "doctor XYZ",
  },
  "proof": {
    ...
  }
}
```

**Figure 5.3.** Example of a Verifiable Credential

Moreover, VCs like diplomas and certificates can be used to authenticate users based on their DIDs. Thus, DIDs and VCs are useful for several aims such as reducing the time and costs of the issuing credential, signing documents or transactions, creating persistent communication channels, sending encrypted private messages, and also log in without usernames and passwords (Mahalle and Shinde, 2021).

#### 5.2.1.4 SSI Architecture

Three fundamental roles that the members of an SSI ecosystem can occupy: issuer, verifier, and holder. These roles and their relations are known as a trust triangle or Verifiable Credential Lifecycle, as illustrated in Figure 5.4, they describe how trust is designed and established in an SSI ecosystem. Thus, these roles are an integral part of the VC standard, they are briefly described below:

- (a) **Issuer:** An entity that provides evidence on a subject in a VC. An issuer sends VCs to holders.

- (b) **Holder:** An entity that requests and receives VCs from issuers and keeps them in a digital wallet or credential repository. Additionally, holders can create Presentations from Verifiable Credentials (VP) and present them to the verifier.
- (c) **Verifier:** An entity that checks, verifies, and confirms holders' attributes and claims that are received in the form of VP from one or more VCs.

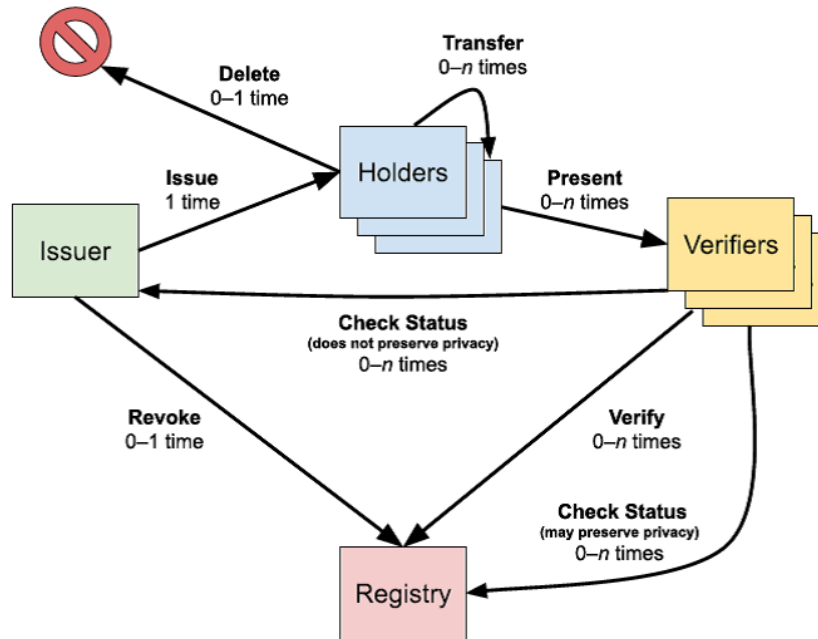


Figure 5.4. Verifiable Credential Lifecycle

According to Figure 5.4, the VC lifecycle illustrates the steps that a VC proceeds through and the roles that are involved in each step. We take an example of using a VC representing a bachelor's degree. The university represents an issuer, an alumnus is considered the holder, and the verifier is a potential employer (Sporny et al., 2019):

- (a) *Issue:* When the alumnus defends his thesis, a VC will be issued by his university based on his own DID. The alumnus keeps the VC in his digital wallet.
- (b) *Transfer:* The alumnus can transfer his VC to another holder for several reasons.

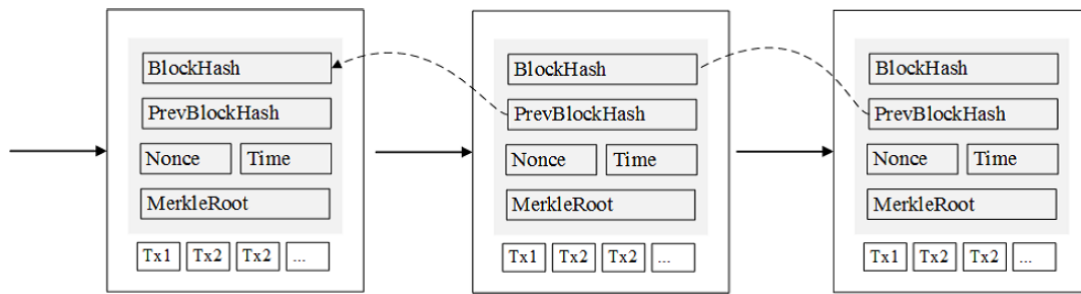
- (c) *Present*: The alumnus must present his VC to the employer which will verify it.
- (d) *Verify and Check Status*: The authenticity of the VC is checked by the potential employer. The employer verifies that the credential is not revoked and meets the standard. To verify the proof, the employer must resolve the DIDs in the credential to a DID document to obtain the public keys. For this reason, the employer must send a query to a data registry.
- (e) *Revoke*: A VC can be revoked and invalidated by the university for some reason.
- (f) *Delete*: A VC can be deleted by the holder from his digital wallet at any time.

### 5.2.2 Blockchain

Blockchain is a distributed database and a public ledger composed of several blocks linked together. Each block is composed of a block header and block data. The block header, as shown in Figure 5.5, contains the block's metadata and a cryptographic link to the previous block's header, whereas the block data contains a set of transactions and other data. The most popular example of blockchain technology-based cryptocurrency is Bitcoin (Nakamoto, 2008), developed and published in 2008 by Satoshi Nakamoto, in his paper titled "Bitcoin: A Peer-To-Peer (P2P) Electronic Cash System" (Nakamoto, 2008). Bitcoin allows P2P transactions without having a trusted intermediary, once the transaction is broadcasted to the network and stored in the chain, it can never be altered or deleted (Nakamoto, 2008). In addition, Bitcoin is based on mechanisms to prevent payment duplication, data modification, and any kind of attacks from malicious users. To achieve these objectives, different technologies are used including digital signatures, public-key cryptography, hashing, and Proof of work.

The most important features of the blockchain are:

- *Immutability*: Blockchain is append-only database technology, i.e. once the data is recorded into the blockchain, it cannot be changed or deleted.



**Figure 5.5.** *Simplified blockchain*

- *Transparency:* It is a crucial feature of the blockchain. Anyone can join the blockchain network, participate in transactions, and view transparent records of transactions.
- *Decentralization:* The blockchain is structured as a peer-to-peer (P2P) network which is fundamentally resilient, decentralized, and open. There are no servers, no centralized services, and no hierarchical structure within the P2P network, all nodes are equal and interconnected.

### 5.2.2.1 Transactions

All the blockchain nodes communicate via transactions. Therefore, the transaction can be defined as a communication form between network nodes, it is generated by a blockchain node, then broadcasted to the network. Each node builds a block of new transactions and then determines the proof-of-work for that block. Once it has the proof of work, it broadcasts the block to every node. Nodes will accept a block only if all the transactions are valid (Yaga et al., 2019). To manipulate transactions on the blockchain, digital wallets are used. By definition, a digital wallet is a software tool that allows users to send transactions and check whether the transaction is confirmed or rejected by the network (Yaga et al., 2019).

### 5.2.2.2 Merkle trees

Each block of blockchain uses Merkle trees to record a summary of all transactions in the block. A Merkle tree is a type of data structure that summarizes and checks the

integrity of big sets of data, as seen in Figure 5.6. Transactions will not be stored in the Merkle tree; rather, their data will be hashed, and the result of the hash will be in each child node. Because a Merkle tree is a binary tree, it needs an even number of child nodes.

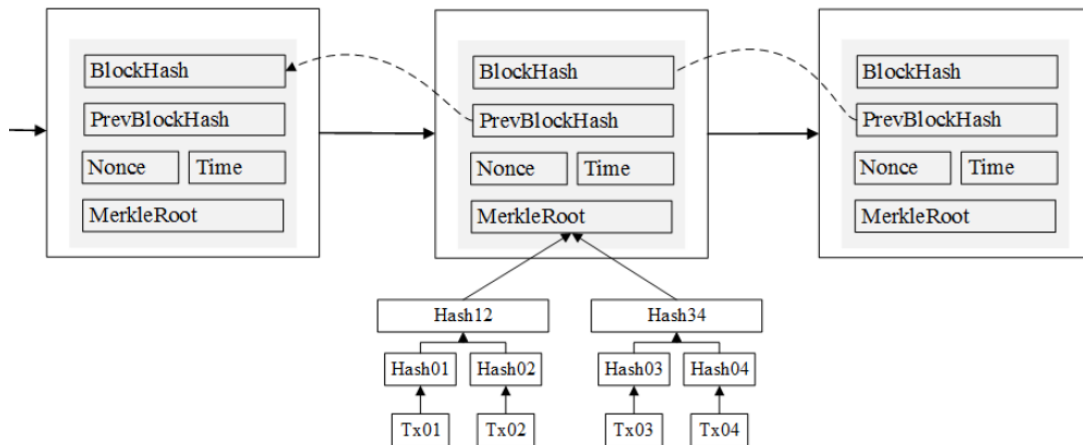


Figure 5.6. Merkle tree

### 5.2.2.3 Consensus mechanism

A consensus algorithm is a process that enables all blockchain network peers to reach a common agreement (consensus) about the current data state of the distributed ledger (Yang and Li, 2020). The consensus algorithm allows the blockchain to achieve reliability and trust among nodes while ensuring security in the network environment. It essentially ensures that each new block added to the Blockchain is the only version of the truth that is accepted by all of the nodes in the Blockchain. Some benefits of the consensus protocol consist of equal rights to every node, collaboration, agreement, and mandatory participation of each node in the consensus process.

Various types of consensus mechanisms exist, and each one functions with different principles.

- *Proof of Work (PoW)*: The PoW consensus algorithm is employed to select a miner for the next block generation. This consensus algorithm is used by Bitcoin, its primary objective is to solve a complex mathematical puzzle that requires a lot of

computational power. As a result, the node that solves the challenge first gets to mine the next block.

- *Proof of Stake (PoS)*: This is the most common alternative to PoW. With POS, nodes validate block transactions based on the number of staked coins instead of purchasing expensive equipment to solve a challenging puzzle. Each validator starts validating the blocks by putting a bet on it if they find the block which they think can be added to the chain. Once the block is added to the blockchain, all validators receive rewards based on their bets and their stakes increase accordingly.

There is a wide variety of other consensus algorithms, each one has its advantages and disadvantages such as *Proof of Capacity (PoC)* which enable contributing nodes on the blockchain network to share resource capacities (memory and hard disk space). A node is given more rights to maintain the public ledger if it has more memory or hard disk space.

The *Proof of Authority (PA)* paradigm is a highly scalable system because it relies on a limited number of block validators. Blocks and transactions are verified by approved participants, they serve as the system's moderators.

The hybrid Proof of Work and Stake system aims to capture the advantages of each approach and use them to balance each other's vulnerabilities.

### 5.2.3 Access control

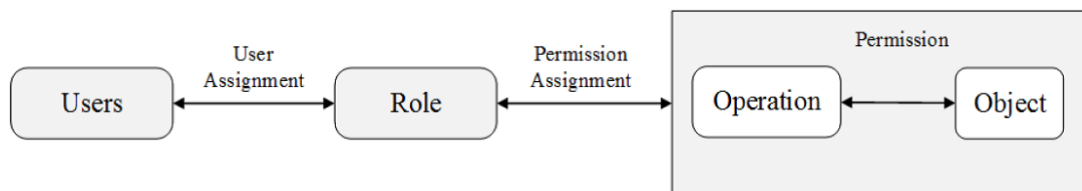
Access control techniques ensure that only allowed parties can access approved data. The access control should be patient-centric, which means that patients have the right to authorize the use and disclosure of their electronic health records. However, access control is an intrinsic issue in the medical environment, due to the various types of medical and non-medical staff involved in the interactions with patients. There are various types of access control systems, among them the following:

### 5.2.3.1 Role-based access control (RBAC)

In 2000, Sandhu et al. formally introduced RBAC which is standardized by ANSI. The following elements represent the main factors of RBAC:

- *User*: the person who interacts with a system.
- *Role*: job function or responsibility within an organization.
- *Permission*: an operation on an object.

RBAC was initially suggested for organizations where authorizations will be allowed to roles rather than individuals. Roles can be created by an organization based on different job functions and responsibilities (e.g., doctor, nurse, emergency medical agent, pharmacist, etc.). Thus, the fundamental idea behind RBAC is that users and permissions can be linked with roles, as shown in Figure 5.7. This concept makes easy the management of permissions by system administrators. However, RBAC is not adequate to incorporate contextual conditions.



**Figure 5.7.** Basic elements of RBAC

In our work, we focus on the simplest model of RBAC, which has the following components (Sandhu et al., 2000):

- $U$  (users),  $R$  (roles), and  $P$  (permissions),
- $PA \subseteq P \times R$ , many to many,  $PA$  (Permissions Assignment),
- $UA \subseteq U \times R$ , a many to many,  $UA$  (users Assignment),

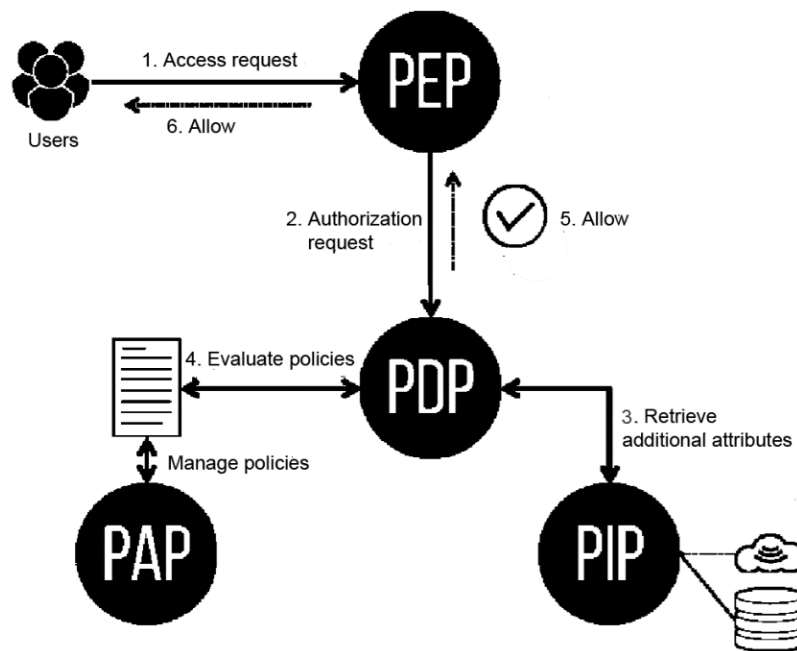
### 5.2.3.2 Attributed-based access control (ABAC)

ABAC is an authorization model that defines and evaluates dynamic and context-aware access control policies according to attributes and conditions. It allows various authorization processes and constraints defined by the relationship between attributes such as physical location, time, resource types, etc. ABAC is built on the three following key elements: Attributes, Policies, and Architecture.

1. **Attributes** Attributes are characteristics given to both subjects and objects. They are key-value pairs where the key represents the identifier of the attribute, used to describe anyone or anything. In addition, attributes can be multi-valued and they are divided into categories:
  - *The subject category,*
  - *The action category,*
  - *The resource category,*
  - *The environment or context category.*
2. **Policies** Policies are a set of rules that specify who may access information under what circumstances, and how access is managed. They combine attributes to express allowed or rejected access. For instance, in an e-health environment, policies might express who is allowed to view, edit, and approve medical transactions.
3. **ABAC Architecture** ABAC architecture is based on the following elements (Brossard et al., 2017), as shown in the Figure 5.8:
  - *The subject (user):* the entity that needs access to a resource,
  - *Policy Enforcement Point (PEP):* receives access requests from users and transmits them to the Policy Decision Point (PDP) to enforce an access control decision (ALLOW or DENY)
  - *Policy Information Point (PIP):* stores the information about the subject's attributes.



- *Policy Retrieval Point (PRP)*: stores and retrieves access control policies, which are managed by the *Policy Administration Point (PAP)*.



**Figure 5.8.** *The ABAC Architecture*

Briefly, Figure 5.8 demonstrates the interactions between different elements of the ABAC system. The access request is intercepted by the PEP, which converts the access request to an authorization request and sends it to the PDP which uses the information provided by the PIP to lookup attributes that are referenced in the policies and needed to decide whether the request should be allowed or not.

### 5.2.3.3 Centralized and decentralized access controls

Access control schemes can be decentralized, centralized, or hybrid. Centralized access control schemes provide access management across systems inside the organization. However, these schemes suffer from a single point of failure issue. Indeed, the decentralized access control model is more evolved and stable than the centralized access control scheme. It is required when multiple elements can grant access permissions to the users. However, decentralized access control systems require more administration and maintenance.

### 5.2.4 Zero-Knowledge Proof (ZKP)

Zero-knowledge proof (ZKP) is proposed by Goldwasser, Micali, and Rackoff in 1989 (Goldwasser et al., 2019). ZKP is a cryptographic technique where the prover can prove to the verifier that he knows a certain value without revealing the actual value.

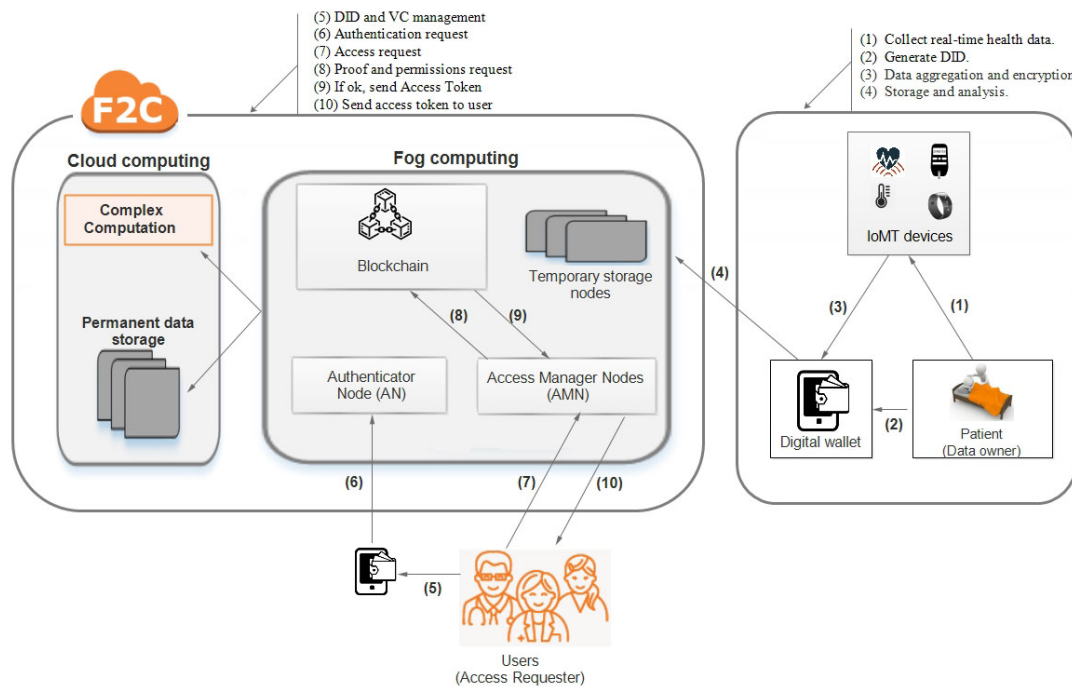
A ZKP system is an interactive protocol in which messages are exchanged between the prover and the verifier for a defined number of rounds using commitment, challenge, and response messages. Initially, the prover generates the first commitment, which is the statement to be proved and sends it to the verifier. Then, the verifier randomly chooses a challenge and sends it to the prover. Finally, the prover calculates the response based on the challenge and sends it to the verifier (Capraz and Ozsoy, 2021).

Whereas, a Non-Interactive Zero-Knowledge Proofs (NIZKP) approach can be used. In this case, the challenge-response process is non-interactive; and a single message will be sent from the prover to the verifier. A NIZKP  $(P, V)$  between a prover  $P$  and a verifier  $V$  for a language  $L$  with a binary relation  $R$  should satisfy the following properties:

1. *Completeness*.  $P$  can convince  $V$  that statement  $x$  is true.
2. *Soundness*.  $V$  can protect himself from being convinced of false statements, except with a very small probability.
3. *Zero-knowledge*. For any statement  $x \in L$ , provided by  $P$ , no information is revealed from  $x$  to  $V$  that it could not compute alone before running the protocol.

## 5.3 Models and security requirements

This section describes the Decentralized Self-Management Access Control (DSMAC) architecture which is depicted in Figure 5.9. In the following subsections, we first present the main components of our system. Then, we discuss the adversary model followed by security requirements and design goals.



**Figure 5.9.** System overview

### 5.3.1 System model

DSMAC is a novel system that presents a decentralized access control scheme based on blockchain and self-sovereign identity (SSI) mechanisms. It is composed of three layers, namely: IoMT devices layer, the user layer, and the F2C layer.

1. **IoMT devices layer** The aims of this layer are sensing, collecting, encrypting, and uploading health data to F2C computing. It is composed of sensors, smart devices, and a digital wallet. Digital wallets are secure digital repositories that enable users to store and manage identifiers and verifiable credentials. The sensors are resource-constrained and have limited resources, the sensed data are sent to the digital wallet for aggregation and encryption purposes.
2. **User layer** In DSMAC, each individual is identified by a DID, and he is characterized by a set of VCs issued by trusted issuers. DSMAC is based on mobile wallets to allow individuals to manage their DID and authorize access to their health data. Furthermore, two main types of users can participate in DSMAC, such as:

- *DO (Data Owner)*: the DO represents the entity that owns the data to be shared like a patient. DO play a vital role in our system, he can manage his digital wallet and perform data encryption, set the access policies, and upload ciphertext of the shared data to the F2C. Also, he can delegate permissions to other users to manage his mobile wallet on behalf of a DID owner. For example, an elderly parent might delegate to an adult the authority to manage the parent's medical account.
- *AR (Access Requester)*: AR is an entity that wants to access data shared by DO. An AR can have different privileges in diverse situations such as a doctor, nurse, pharmacist, and researcher. Each AR must create his DID using the digital wallet, then register in the system using his DID. The AR initiates a data access request, obtains authorization and the URL of the data location, then downloads data ciphertext from the F2C according to the URL.

3. **F2C computing layer** This layer comprises two sub-layers, fog computing, and cloud computing. It combines the advantages of both, and it is detailed in our previous work (Saidi et al., 2020).

(a) Fog computing:

Fog is located close to the end-user to satisfy the low latency and high scalability requirements of the IoMT scenario. The main components of this sub-layer are:

- *Temporary storage*: which represents the off-chain storage and periodic data will be sent to cloud computing for permanent storage. However, health data are neither stored nor processed on-chain to avoid potential high load, it will be stored temporarily at the fog layer to have real-time medical data access with minimal latency.
- *Blockchain-based Decentralized Access Control*: blockchain is used to store the users' public key, decentralized policies, and the user's proof to

verify the user's credentials with minimum time and cost. It includes several nodes responsible for mining the blocks and executing the smart contract used to ensure secure and reliable access to medical data. Also, blockchain is based on the Proof of Authority (PoA) consensus algorithm to increase throughput and reduce the system latency (Yang et al., 2022).

- *Authorization Management Node (AMN)*: AMN is responsible to manage the relationships between AR and permission assignment according to his role or his attributes. Therefore, it acts as a gateway between the blockchain and the user layer.
- *Authenticator Node (AN)*: AN manages AR authentication by verifying his DID and VCs.

(b) Cloud computing:

We integrate cloud computing into our DSMAC framework because of its strong capacity for computation and storage (Liu et al., 2021). It includes (i) Complex computation to perform the complex analyzes that could not be done in fog computing. (ii) Permanent storage to store permanently the history of medical data.

### 5.3.2 Adversary model

This sub-section discusses the security, and privacy-preserving medical data issues as well as the DSMAC reliability. To satisfy the goal of preserving privacy and resisting attacks threatening access authorization, we suggest some security assumptions. Then, we describe some attacks aimed at obtaining access authorization to medical data generated.

The end-users are assumed to be honest but curious to get more data than what their access privileges allow. For example, a pharmacist can be interested in obtaining patient prescriptions and learning different doctors' prescription patterns which could be useful for marketing purposes. Additionally, we assume that the fog's nodes are

honest but curious. They can execute their assigned tasks but are curious about the privacy of the IoMT devices which are usually exposed to malicious attacks. Thus, attackers might be present between the IoMT devices and the fog storage node to establish a channel through which different components seem to communicate directly. They will also try to satisfy the access policies by obtaining or using attributes illegally. They can control, monitor, and modify all the data, tamper with the message, drop some packets and even replace the original message. In short, all the data transmitted to the fog storage and the blockchain through the digital wallet can be intercepted and analyzed by the adversary. For this reason, we are interested only in attacks threatening the access process such as:

#### **5.3.2.1 Replay attack**

An attacker can observe and record some encrypted data during the transmission and reply to them in another request using the user's signature. The attacker can act as a user and actively interact with the system to get the messages, or he can be a passive observer who collects the messages at the network level (Sonnino et al., 2020). Therefore, this attack can help to get illegal authorization in the DSMAC framework.

#### **5.3.2.2 Spoofing attack**

The spoofing purpose is to gain access to health records using another user's credentials and steal the personal information related to the authorized user (van der Merwe et al., 2018). Thus, this attack is the act of disguising an identity so that it appears to be associated with a trusted and authorized user, the adversary forges the credentials of the data owner and tries to communicate with the system. During this attack, we have considered the case where an attacker spoofs a user DID to gain access to medical data. Furthermore, he may change the identity of the data owner.

### 5.3.2.3 Credential-stuffing attack

This attack is based on the assumption that many users reuse their usernames and passwords across many services. Thus, attackers exploit lists of compromised user credentials to get access to a system. This attack is the automated injection of stolen credentials to fraudulently gain access to user accounts (Rees-Pullman, 2020).

### 5.3.3 Security requirements and design goal

The main security requirements to be satisfied in DSMAC scheme are summarized as follows.

- *Patient privacy.* Any user who does not have enough attributes to fulfill the access policy must be prevented from accessing the patient health data. So, it is critical to avoid any sort of illegal sharing of patients' personal data.
- *Access control:* Access control systems define who can access the patient's data and which part(s) of the data can be accessed, to ensure that only allowed parties can gain access to authorized data (Sookhak et al., 2021). So, access control is a critical problem due to the different kinds of end-users involved in the interactions between patients and healthcare systems.

Our design goal is to propose a privacy-preserving medical information scheme based on a decentralized access control system, blockchain, Decentralized Identifiers (DIDs), and verifiable credentials (VCs). Our framework provides the opportunity to share medical data and define access rights by the patient for giving access to different end-users without having a central authority. Hence, the following issues will be addressed:

- How to acquire a decentralized access control system?
- How can end-users access medical records?
- Can the DID approach add privacy value to the system?

## 5.4 Proposed DSMAC scheme

This section presents our DSMAC model that ensures decentralized access control techniques in the healthcare environment by integrating SSI technology with blockchain. The main goal is to achieve data privacy using access control methods based on blockchain, DID, and VC.

### 5.4.1 Towards a decentralized access control scheme

Our model proposes a novel decentralized access control method that reuses concepts and mechanisms of Role-based access control (RBAC) (Cruz et al., 2018) and Attribute-based access control (ABAC) (Song et al., 2020), permitting the owner to self-manage his access control policies. Hence, DSMAC is based on the user's role, attributes, and contextual constraints. In a regular case, it assigns default permissions (DP) to ARs using the RBAC system. In cases where Data Owner (DO) is confronted with an emergency case, our model will assign adaptive permissions (AP) to ARs based on a set of contextual attributes using the ABAC system.

Consequently, we can define users' permission policies (P) as the following:

$$P = DP \cup AP \quad (5.1)$$

#### 5.4.1.1 Role-Based Decentralized Access Control (RDAC)

As discussed in the previous sections, RBAC defines how a user can access data, allowing read-only or read/write permissions to different roles. In the DSMAC framework, we present the Role-based Decentralized Access Control (RDAC) scheme that integrates the RBAC model into the Blockchain. The main goal of the RDAC approach is to assign roles to ARs based on their VCs for accessing or updating medical data, then define the rules that must be followed. Later, all the access control policies



are managed by a smart contract according to the user-role assignments, and each user can be assigned to one or multiple roles.

In summary, roles are associated with default permissions, the default permissions are granted to users, and defined by the Policy Decision smart Contract (PDC).

**Definition 2** Default Permissions (DP) represent the regular basic permissions (RP) that are defined explicitly by a smart contract based on the user's role (R).

$$DP \subseteq R \times RP \quad (5.2)$$

Default permissions include the patient's DID, the off-chain URL of medical data, the role of AR, and authorized permission (Read, Write, and Update).

#### 5.4.1.2 Attributes-based Decentralized Access Control (ADAC)

Despite ABAC being one of the most popular access control methods, it has serious privacy issues (Song et al., 2020). In the DSMAC framework, we propose the Attributes-based Decentralized Access Control (ADAC) model that combines the ABAC with the SSI technology to solve the issue of privacy. We implement the access control policies based on DID Document (DDO) to provide a level of adaptive security that would meet the DO's needs in emergency cases. The access permissions are granted to users through the subject's attributes, object's attributes, or environment attributes (Song et al., 2020). Therefore, the DO can enforce the default permissions (DP) by configuring Adaptive Permissions (AP) based on DO's attributes, AR's attributes, and certain contextual attributes which must satisfy specific requirements to perform a specific operation. A contextual attribute defines a specific environmental characteristic whose real value changes dynamically such as date, time, location, and health status (emergency case, critical crisis, normal, etc.). Hence, AP is introduced to configure decisions locally for emergency and unanticipated cases. Additionally, blockchain technology is integrated with the ADAC model to improve and enhance security and data privacy. The patient's wallet creates access control policies and stores

them in the DDO. The wallet broadcasts the DDO as a transaction to the network; the network verifies, validates the transaction, and adds it to the blockchain. DSMAC system enables the patient to quickly modify permissions by changing contextual information.

**Definition 3** Adaptive Permissions (AP) are defined to suit contextual constraints (CC) and relevant contextual conditions (CD) confronting DO (e.g. crisis, emergency, a heart attack, an allergic reaction, etc.).

$$AP \subseteq R \times CC \text{ where } R = \text{role} \quad \text{and} \quad CC = \text{set of } CD \quad (5.3)$$

AP becomes active when an emergency has been declared, and a subset of the contextual conditions 'CD' is satisfied. The set of contextual conditions can be combined based on the context information and using conjunction ( $\wedge$ ), disjunction ( $\vee$ ), and negation ( $\neg$ ) operators.

For example, we consider the following contextual conditions (CD): 'T' denotes a request Time, 'A' denotes a location Address and 'S' denotes a health Status. Contextual conditions are formed by making conjunctions of these elements (eq. 5.4).

$$CD = \{(\dots, (A \wedge S), (T \wedge A), \dots) \mid cd \in CD\} \text{ e.g. : } cd1 = A \wedge S \quad (5.4)$$

### CASE STUDY:

We assume that a patient suffers a serious medical emergency as a result of an accident, and he needs prompt intervention by medical professionals. The patient's digital wallet can allow users to quickly reach the emergency case, it will make access to medical records easier and faster. Thus, according to the contextual constraints mentioned in (eq. 5.4), the patient or his delegate will approve the adaptive permissions for a user if the following contextual conditions are satisfied:

1. *cd1: the doctor is not far from the 'accident scene'.*
2. *cd2: if the patient's health status is in a 'critical' condition.*

$$if (AR(user) \wedge role(doctor)) \wedge (cd1 \wedge cd2) \text{ then } Approve \text{ access} \quad (5.5)$$

Once the doctor leaves the ‘accident scene’ or the patient’s health status becomes ‘normal’ again, the adaptive permission will be deactivated.

## 5.4.2 Decentralized Access Control Scheme Based-SSI model

In this section, we propose a privacy-preserving medical data-based SSI technology to improve user authentication and authorization mechanisms and deliver enhanced interoperability (Lim et al., 2022).

### 5.4.2.1 DID approach

DIDs represent a Decentralized Identifier of a subject. They are generated by the user (DO and AR) using the public/private key pair (Ehret et al., 2021) and signed with the user’s private key. To implement a DID, we should specify the DID method which is composed of a method scheme and operations. The method scheme specifies the structure of the DID implementation’s string identifier. Operations define how to create, read and verify a DID document, as well as how a DID controller can resolve or update a DID document (Sporny et al., 2022).

In our system, we have used the term “dac” (Decentralized Access Control) to identify the method name. Thus, All DID must begin with the following prefix: “did:dac:”. The remainder of the DID, after the prefix, is the Method-Specific Identifier (MSI) (Sporny et al., 2022), which produces a string identifier of the form “did:dac:namespace”. The different steps carried out by the user using the digital wallet are:

1. Generate public and private keys then the DID.
2. Request for issuance of verifiable credentials, accept the issued credentials then store them.

3. Receive a request from a verifier for proof of one or more credentials.
4. Data aggregation, encryption, and signature.
5. Create Access Control policies.

Therefore, the process of the DSMAC protocol-based DID approach is as follows: First, each user (DO, AR) must create his DID using the digital wallet, then, he sends a signed request for issuing a new credential. When the issuer (e.g. hospital) receives the request, he checks the validity of the request by verifying the AR's signature. Once the verification is completed, the issuer agrees to the credential request and issues VC. The VC will be stored in the user's wallet.

Later, the AR must authenticate using his DID before submitting an access request. When an authentication request is sent, the Authenticator Node (AN), which acts as a verifier, transmits a proof request to verify the AR identity. The AR processes the proof request and determines the necessary credentials to satisfy the proof based on ZKP (Capraz and Ozsoy, 2021), then he sends the response to the AN. After, the AN uses the issuer DID and the credential definition specified in the proof response to verify the response. If the response is validated, then, token-based authentication is submitted to the AR. The flowchart shown in Figure 5.10 describes the interactions between DO's wallet, AR's wallet, issuer, and blockchain to manage the SSI's standard.

#### **5.4.2.2 DID Document (DDO) approach**

DID can be resolved by the digital wallet to a standard resource named DID document (DDO) without reliance on a centralized network component. DDO can be stored in the blockchain so that issuers or verifiers can easily find it. DDO contains several components (Sporny et al., 2022), as illustrated in Figure 5.11, "id" denotes the DID, "Publickey" represents one or more public keys that authenticate the DID subject, "Authentication" is used to specify the method that is expected to prove the DID owner, "Service" contains one or more service endpoints that are used to describe how to communicate with a DID owner (Preukschat and Reed, 2021), "Timestamp" indicates when the DDO was created or updated, and "signature" for verifying the

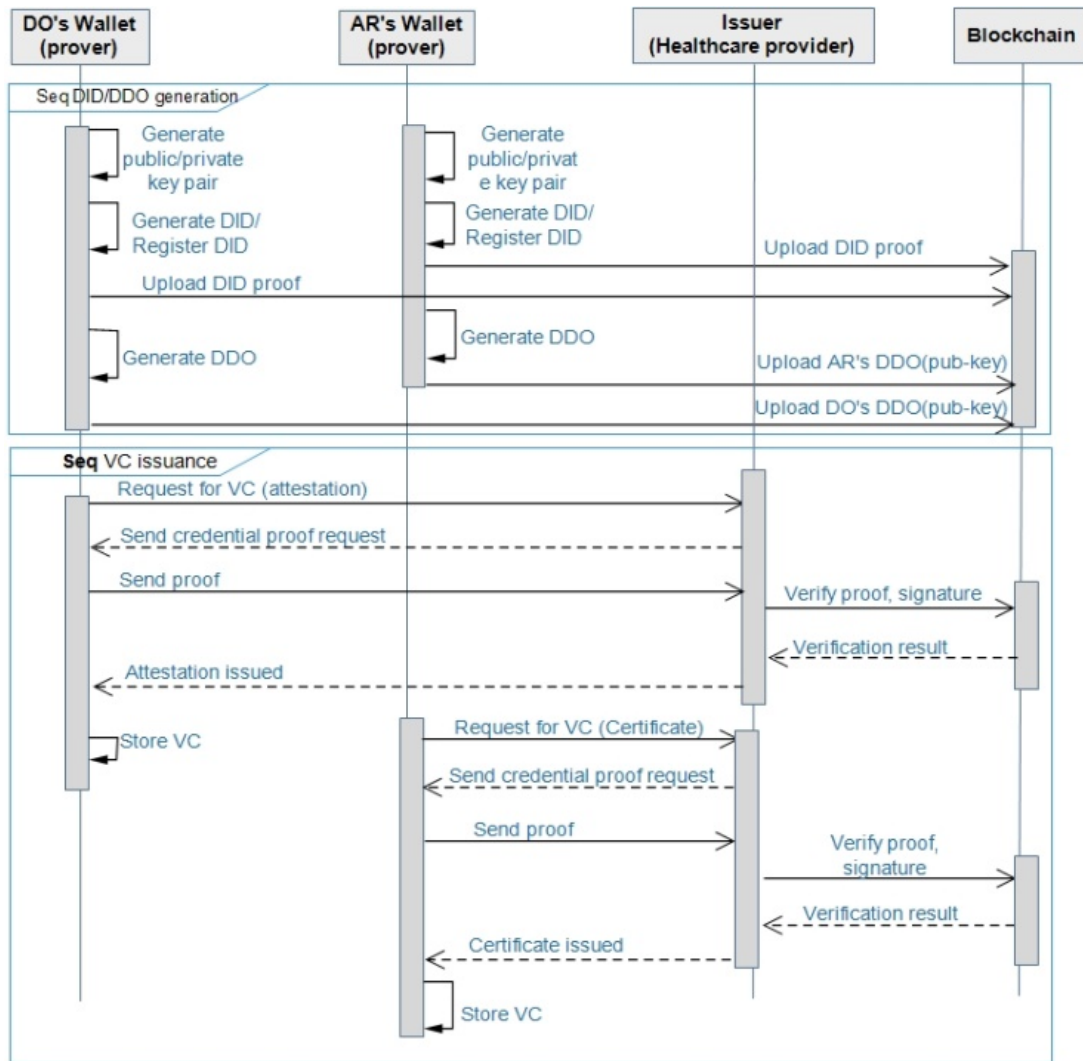


Figure 5.10. Sequence diagram of DID generation and VC issuance operations

integrity of the DDO (Mahalle et al., 2020). These components are necessary to check the user’s identity and the security of their requests. In the DSMAC system, the DDO structure includes a public key and service endpoints which are crucial to accomplish decentralized access control.

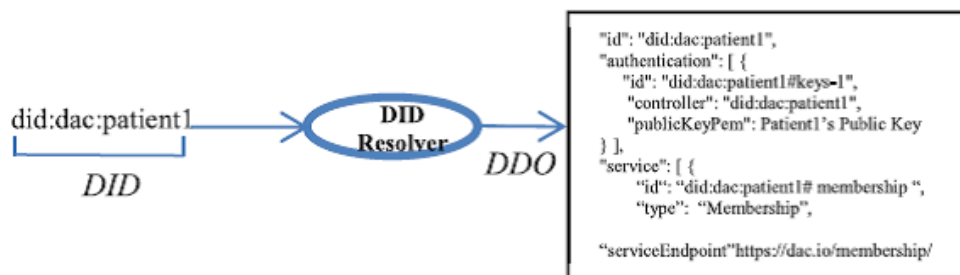


Figure 5.11. The structure and resolution of DID Document (DDO)

### **5.4.2.3 Outsourcing encryption approach**

DSMAC framework includes a mobile application component that enables the users to manage their wallets and the security of their medical data using an encryption scheme. For this reason, a Zero Knowledge Encryption technique is adopted to address specific requirements focusing on data privacy. The data will be encrypted using a mobile app before being sent, and the attackers will only gain access to the encrypted data which is useless without the keys to decrypt it.

### **5.4.3 Decentralized Access Control scheme using Blockchain-based SSI model**

To store the public keys, decentralized policies, and the user's proof, blockchain technology is used and integrated into the DSMAC framework. It is operated on the fog layer to provide low latency for decentralized access control functions (Saidi et al., 2020). Additionally, DSMAC is based on SSI to facilitate user authentication and authorization in regular and emergency cases.

#### **5.4.3.1 RDAC-based Policy Decision smart Contract (RDAC-PDC)**

The RDAC-PDC model is used to define, manage, and store default permission policies (DP) based on the RDAC approach and using the features of the smart contract. To reach these goals, a policy decision smart contract (PDC) was developed. PDC is designed to assign user-role along with role permission, then publish the details on the blockchain. The main features of the PDC are:

1. Allow the verifier (hospital) to check the user's role based on his credentials.
2. Allow the patient to permit end-users to access his medical data based on their associated roles and credentials.
3. PDC implements several functions to make the user-role assignment efficient, effective, and secure.

Moreover, the Authorization Management Node (AMN) is used as the agent who manages the request access and interacts with PDC using the Request Access transaction. Figure 5.12 describes the sequence diagram of the RDAC-PDC scheme.

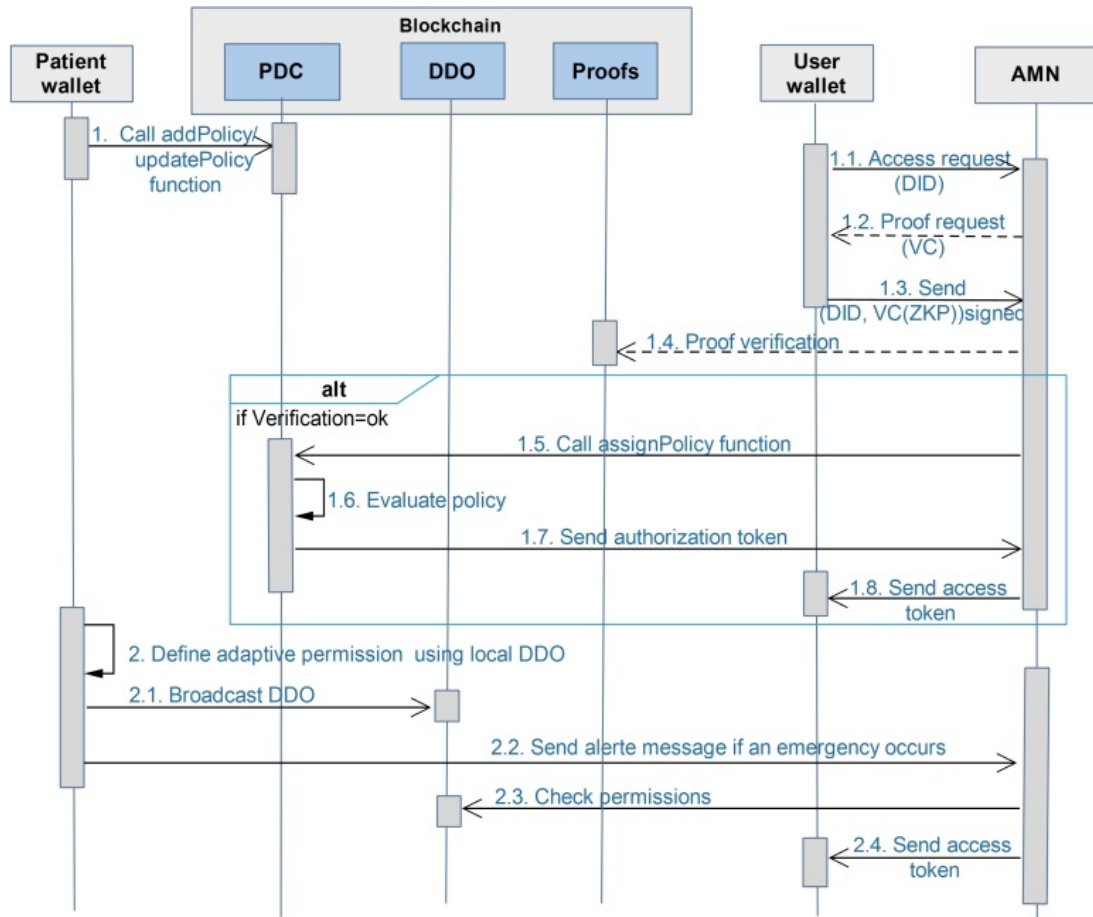


Figure 5.12. Sequence diagram of RDAC-PDC approach

1. After a successful authentication step, the AR sends an access request to AMN by enclosing his DID.
2. AMN sends a proof request to AR.
3. AR generates a payload based on his DID and VC protected by the ZKP technique, then, signs the payload with his private key and sends it to the AMN.
4. To verify the validity of the payload, AMN checks the signed payload with AR's public key stored in the blockchain.
5. After the payload and role-checking step, the AMN redirects the request to the PDC as a transaction.

6. If the AR's attributes and the policy attributes in the PDC are similar, then the PDC will create an authorization token that includes the access permissions of the AR and the transaction will be recorded in the blockchain.

#### 5.4.3.2 ADAC-based DID Document (ADAC-DDO)

Managing medical data access and defining security policies becomes more critical and complex in an emergency case since the access does not only depend on the user's role but it's also attached to contextual constraints. In the DSMAC framework, the patient plays a huge role in emergency cases. He can enforce the default permissions (DP) by configuring adaptive permissions (AP) based on both AR and DO attributes using DID Document (DDO).

DDO contains several fields like the context, authentication mechanism, user's digital signature, and service definition. Each service has its id and type, as well as a service Endpoint with a URL or further properties describing the service. The id is used to identify the service itself, while the service endpoint URL is used for the outside service caller (Sporny et al., 2022). To configure the DDO permissions, AMN sends an authorization request to the blockchain once receiving an alert message from the patient's wallet. So, according to the patient DID included in the authorization request, the blockchain returns the corresponding authorizations managed by the patient's DDO. Then, AMN sends an access token to users mentioned in the Membership service if and only if they fulfill the conditions. As defined in listing 1, we have used the service endpoint to express adaptive access control policies (AP). We define the access privileges' URL based on both "Membership" and "Permission" services. The "Membership" service maintains a list of DIDs of the authorized users. Each user must be a member of one or more of the following roles: "doctor, pharmacist, and researcher". Likewise, the "Permission" service specifies the access control policies of the user managed by the "Membership" service. Moreover, access policies are composed of one or several statements; each statement includes information about



single adaptive permission (AP). The information in a statement is contained within a series of elements:

1. **User** – Indicates a list of DID of the accepted user: *“user” : [“did:dac:alice” ]*,
2. **Role** – Indicates a list of authorized roles: *“role” : [“doctor”]*,
3. **Rules** – composed of the following items:
  - **grant**: *“grant” : [“read”, “write”, “update”]*,
  - **by**: Specifies the user’s name and role to which we would like to give access rights: *“by” : [“alice\_u:doctor\_r”]*,
  - **when**: Specifies the circumstances under which the policy grants permission: *“When”:[“time = 08pm - 10am”, “status = emergency”]*,
  - **url**: Includes the URL of health records to which the actions apply. *“url” : [“fog.storage.patient1.emg\_data”]*,

To specify the user’s name and role to which we would like to give access rights, the DDO policies are based on hierarchically-named attributes, where ‘u’ means user, ‘r’ means the role, and ‘t’ means type, separated by the ‘:’ character.

**For example**, *“alice\_u:doctor\_r:cardiologist\_t”* means that the user Alice must be a doctor with a cardiologist specialty. If “Alice” is in the “Membership” service, the patient or his delegate can approve write and update permissions for “Alice” if the following contextual conditions are satisfied:

1. Alice’s role is “doctor”.
2. She is not far from the “accident scene”.
3. If the patient’s health status is critical”.

**Listing1: patient DDO structure based ADAC-DDO**


---

```

{"id": "did:dac:patient1",
 "authentication":
 [ {
   "id": "did:dac:patient1#keys-1",
   "type": "RsaVerificationKey2022",
   "controller": "did:dac:patient1",
   "publicKeyPem": Patient1's Public Key
 } ],
 "service":
 [ {
   "id": "did:dac:patient1# membership ",
   "type": "Membership",
   "serviceEndpoint" : https://192.168.0.100/membership/,
   "user" : ["did:dac:alice", "did:dac:bob", "did:dac:eve"],
   "role" : ["doctor", "nurse", "pharmacist", "researcher"]
 },
 {
   "id": "did:dac:patient1# permission ",
   "type": "Permission",
   "serviceEndpoint" : https://192.168.0.100/permission/,
   "rules":
 [ {
   "grant": ["write", "update"],
   "by": ["alice_u:doctor_r"],
   "When" : ["location= accident_scene ", "status=emergency"],
   "url" : ["fog.storage.patient1.emg_data"]
 },
 {
   "grant": ["read"],
   "by": ["eve_u:pharmacist_r"],
   "When" : ["time= 09pm-09am ", "status=critical"],
   "url" : ["fog.storage.patient1.prescription_emerg_data"]
 } ]
 } ]
 } ] ]

```

---

**Table 5.1.** *Tools used in the experimentation*

| <b>Tools</b>             | <b>Description</b>  |
|--------------------------|---|
| Hyperledger Indy         | A permissioned blockchain, used to create and control digital identities.   |
| Hyperledger Ethereum     | is a public blockchain used to build decentralized applications (dApps) and smart contracts.  |
| Hyperledger Aries        | It serves as the infrastructure for transaction interactions, it provides tools to transmit, verify, and store digital credentials.                                   |
| Aca-py                   | Aries-CloudAgent-python is a python application that serves as a cloud agent interface to both the ledger and external holders, it interacts with other Aries agents. |
| Von-network              | Verifiable Organization Network is a set of tools for building decentralized identity systems using the Hyperledger Indy.   |
| Docker community edition | is a tool that simplifies the process of deploying applications by using containers.  |
| Postman API Network      | Provides a user interface for creating and sending API requests.  |

## 5.5 Experiments and Results

### 5.5.1 Experimental setup

To evaluate the performance of DSMAC, the hyperledger Indy (Banerjee et al., 2022) and hyperledger Aries (Manoj et al., 2022) are deployed. The set of tools used in the experiments is described in table 5.1.

In the general setup of the DSMAC framework, Docker is used to build and run the system test setup. We utilized the Admin UI from the VON network repository to connect to the Indy network and control different nodes (Ferdous et al., 2023). VON network initiates the Hyperledger Indy with the genesis block, a server, and 04 nodes, as illustrated in Figure 5.13(a). All involved agents (issuers, holders, and verifiers) must be registered in Hyperledger Indy and provided with the DID. To check and display the configuration, we can consult the web page: <http://localhost:9000>, as shown in Figure 5.13(b).

Also, we have used the ledger browser to generate DID for different agents, as shown in Figure 5.13(c) by using the default option “Register from seed” in the “Authenticate a New DID” section. Once this step is successful, detailed information such as Seed, DID and Verkey will be shown below the “Register DID” button, as illustrated in Figure 5.13(c).

In addition, four agents (patient, doctor, nurse, and hospital) have been implemented using the hyperledger Aries, as illustrated in Figure 5.14. Those agents are capable of connecting to the Indy network and generating transactions. They are written in Python using the ACA-Py library which will be run over Docker, as shown in Figure 5.15. The ACA-PY provides a queue to hold messages until the mobile agent requests them because the mobile wallets are not online at all times, and are not constantly polling to see if they have any incoming messages (Ferdous et al., 2023).

```
Using: docker-compose --log-level ERROR

Starting von_node3_1      ... done
Starting von_node4_1      ... done
Starting von_webserver_1 ... done
Starting von_node2_1      ... done
Starting von_node1_1      ... done
Want to see the scrolling container logs? Run "./manage logs"
```

(a) Starting Von Network

The screenshot shows a web interface for managing the Von Network. At the top, there is a search bar with 'localhost:9000' and a list of browser tabs including 'Red Hat Products Docu...'. Below this, four nodes are listed, each with a circular icon and detailed information:

- Node1:** DID: 8ECVsk179mjsjKRLWiQtssMLgp6EPHwXtaYyStWPSGAb, Uptime: 3 hours, 2 minutes, 9 seconds, Txns: 0 config, 104 ledger, 4 pool, 0.00805/s read, 0/s write, indy-node version: 1.12.4
- Node2:** DID: 8ECVsk179mjsjKRLWiQtssMLgp6EPHwXtaYyStWPSGAb, Uptime: 3 hours, 2 minutes, 9 seconds, Txns: 0 config, 104 ledger, 4 pool, 0.00650/s read, 0/s write, indy-node version: 1.12.4
- Node3:** DID: DKVxG2fXXTU8yT5N7hGEbXB3dfdAnYv1JczDUHpmDxya, Uptime: 3 hours, 2 minutes, 10 seconds, Txns: 0 config, 104 ledger, 4 pool, 0.00467/s read, 0/s write, indy-node version: 1.12.4
- Node4:** DID: 4PS3EDQ3dW1tci1Bp6543CfuuebjFrg36kLAUcsgfaA, Uptime: 3 hours, 2 minutes, 10 seconds, Txns: 0 config, 104 ledger, 4 pool, 0.00787/s read, 0/s write, indy-node version: 1.12.4

(b) Management page

The screenshot shows a web form titled 'Authenticate a New DID'. The form includes the following elements:

- Header: Authenticate a New DID
- Instruction: Easily write a new DID to the ledger for new identity owners.
- Options:  Register from seed,  Register from DID
- Field: Wallet seed (32 characters or base64) with value: EmatiSaidi0000000000000000002022
- Field: DID (optional)
- Field: Alias (optional)
- Field: Role (dropdown menu) with value: Endorser
- Button: Register DID
- Success Message: Identity successfully registered:
- Output: Seed: EmatiSaidi00000000000000000000002022, DID: AQmsoEh9YdVbXQNYsr84zy, Verkey: 68Tz2ejL6wCQcnjhXt8zwGQ6aFHcmBp9VsojUsREterH

(c) Agent DID registration

Figure 5.13. VON network

```

:.....:
: Patient :
: :
: Inbound Transports: :
: :
: - http://0.0.0.0:8000 :
: :
: Outbound Transports: :
: :
: - http :
: - https :
: :
: Public DID Information: :
: :
: - DID: :
: :
: Administration API: :
: :
: - http://0.0.0.0:11000 :
: :
: :
: ver:0.7.4-rc2 :
:.....:

```

**Figure 5.14.** Running of ACA-Py agent (Patient)

The library ACA-Py provides all the Aries functionality such as interacting with the ledger and other agents, managing secure storage, sending event notifications, and receiving instructions from the controller (Ferdous et al., 2023). Therefore, the ACA-PY component is necessary to securely deliver medical data from the wallet to the F2C infrastructure. Therefore, another layer of encryption is added for each agent (Ferdous et al., 2023).

```

$ docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                               NAMES
185ea2856aab   aries-cloudagent-runner             "/bin/bash -c 'aca-pr"   About a minute ago   Up About a minute   0.0.0.0:6543->6543/tcp             aries-cloudagent-runner_dqyyZ26Xiuodh1w5
0763d75599b3   docker-tails-server                "/bin/bash -c 'tailsr"   59 minutes ago     Up 59 minutes     0.0.0.0:4044->4040/tcp             docker-tails-server_1
037546914ef0   wernight/ngrok                      "ngrok http tails-ser"   59 minutes ago     Up 59 minutes     0.0.0.0:4044->4040/tcp             docker-ngrok-tails-server_1
F5e44dfabfda   von-network-base                    "bash -c 'sleep 10; r"   About an hour ago   Up About an hour   0.0.0.0:9000->8000/tcp             von_webserver_1
F6ac6a3a0f5c   von-network-base                    "bash -c './scripts/r"   About an hour ago   Up About an hour   0.0.0.0:9703-9704->9703-9704/tcp   von_node2_1
e828e09be2e9   von-network-base                    "bash -c './scripts/r"   About an hour ago   Up About an hour   0.0.0.0:9701-9702->9701-9702/tcp   von_node1_1
b4de7642f01f   von-network-base                    "bash -c './scripts/r"   About an hour ago   Up About an hour   0.0.0.0:9707-9708->9707-9708/tcp   von_node4_1
b73b32bcb28b   von-network-base                    "bash -c './scripts/r"   About an hour ago   Up About an hour   0.0.0.0:9705-9706->9705-9706/tcp   von_node3_1

```

**Figure 5.15.** Docker list containers

Moreover, we have used Postman API for representing digital wallets. Postman is organized into several collections and API which is composed of a set of actions performed by the agents. Figure 5.16 illustrates the Patient\_Emergency case which details the process followed in the case of an emergency.

POST http://localhost:11000/connections/create-invitation

Params Authorization Headers (8) Body Pre-request Script Tests Settings

Query Params

| KEY | VALUE | DESCRIPTION |
|-----|-------|-------------|
| Key | Value | Description |

body Cookies Headers (4) Test Results 200 OK 505 ms 874 B

Pretty Raw Preview Visualize JSON

```

1  {
2    "connection_id": "56f90fd4-f4e6-4627-83e2-12e40f144618",
3    "invitation": {
4      "@type": "did:sov:BzCbsNYhMrjHiqZDTUASHg:spec/connections/1.0/invitation",
5      "@id": "04881c75-1d0e-459c-9d1f-14714f91d932",
6      "serviceEndpoint": "http://172.17.0.1:8080/",
7      "recipientKeys": [
8        "Dg8STC8H21zUSAhYZKyEmdmMLGUCZCEqGYtwgCqjvM45"
9      ],
10     "label": "patient"
11   },
12   "invitation_url": "http://172.17.0.1:8080/?c_i=eyJAdHlwZSI6ICJkaWQ6c292OkJ6Q2JzTl1oTXJqSG1xWkRUVUFTS6c7c3B1Yy9jb25uZWNOaW9ucy8xLjAvb1IsICJAaWQ1OjA1MDQ4ODFjNzUtMmQwZS00NTIjLTI1LkMYWYtMTQ3MTRmOTFKOTMyIiwgInN1cnZpZV9mRmRwb2luZiQzMTcudC1E2Ii4uOjE4MFAA:TFurtTn1V73ucWVudE+1cVM4f0tTb0n01M10-hTM-4E4VNR0-cE1-cE1EhM0+T1h4"

```

(a) Call API: create an invitation in an emergency case

GET http://127.0.0.1:3000/records/emergency/AQmsoEh9YdVbXQNYsr84zy

Params Authorization Headers (8) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

1

Body Cookies (1) Headers (7) Test Results 200 OK 1

Pretty Raw Preview Visualize JSON

```

37  -->
38
39
40  <tr>
41    <td>14-06-2022</td>
42    <td>mal de tete</td>
43    <td>paracetamol 500</td>
44    <td>AQmsoEh9YdVbXQNYsr84zy</td>
45  </td>
46  <div style="float:left">

```

(b) API response in the emergency case

Figure 5.16. Postman API

Furthermore, the main transactions maintained in the ledger have the type NYM, ATTRIB, SCHEMA, and CRED\_DEF, as illustrated in Figure 5.17(a,b,c,d), respectively.

- NYM transaction is used to create DID.

- To add an attribute value to the NYM record, the ledger makes use of ATTRIB transaction.
- SCHEMA transaction generates a template with the required attributes for issuing the credentials to the user/holder.
- The CRED\_DEF transaction defines a credential with user-specific values inserted into the schema in the form of a public key.

In addition, our framework proposes a procedure for integrating Ethereum smart contract-based credential verification into hyperledger Indy. The smart contract is charged with verifying the credentials (role) presented by users and granting access according to the access policies defined by the patient. Hyperledger Indy is used to confirm the validity of the user’s credentials.

```

Message Wrapper
Transaction ID: 5d39cfc525c6e2431e262b5413c7a26fc49c9cae5ce01baac687599defbd0d9
Transaction time: 6/18/2022, 12:35:09 PM (1655552109)
Signed by: V45GRU86Z58d6TV7PBue6f

Metadata
From nym: V45GRU86Z58d6TV7PBue6f
Request ID: 1655552109222177000
Digest: fb394e08577c43271c27549d89c43539a978901b07a21da5fb725607137ad6e6

Transaction
Type: NYM
Nym: A0msoEh9YdVbXQNYsR84zy
Role: ENDORSER
VerKey: 68Tz2ejL6Wc0CnjhXt8zwG06aFhcm8p9VsojUsREterH
    
```

(a) NYM Transaction

```

Message Wrapper
Transaction ID: A0msoEh9YdVbXQNYsR84zy:1:b6bf7bc8d96f3ea9d132c83b3da8e7760e420138485657372db4d6a981d3fd9e
Transaction time: 6/19/2022, 5:45:44 PM (165657144)
Signed by: A0msoEh9YdVbXQNYsR84zy

Metadata
From nym: A0msoEh9YdVbXQNYsR84zy
Request ID: 165657144619501000
Digest: bbd7994308037625595c6738e065bf7bb1855ca48a72fa9b063fa51c7f122f4

Transaction
Type: ATTRIB
Nym: A0msoEh9YdVbXQNYsR84zy
Attribute data: {"endpoint":{"endpoint":"http://localhost:8000/"}}
    
```

(b) ATTRIB transaction

```

Message Wrapper
Transaction ID: A0msoEh9YdVbXQNYsR84zy:2:doctorpass:1.0
Transaction time: 6/19/2022, 12:18:04 PM (1655637484)
Signed by: A0msoEh9YdVbXQNYsR84zy

Metadata
From nym: A0msoEh9YdVbXQNYsR84zy
Request ID: 1655637484960894700
Digest: 6234d730b3c3fcc77d2e441546128de8dc0ed06d3141c208b7a5fd2a495a08a2

Transaction
Type: SCHEMA
Schema name: doctorpass
Schema version: 1.0
Schema attributes:
  • identifiernumber
  • birthplace
  • birthyear
  • birthday
  • firstname
  • lastname
  • birthmonth
    
```

(c) SCHEMA transaction

```

Message Wrapper
Transaction ID: A0msoEh9YdVbXQNYsR84zy:3:CL:61:doctorCredential
Transaction time: 6/24/2022, 1:23:10 AM (1656030190)
Signed by: A0msoEh9YdVbXQNYsR84zy

Metadata
From nym: A0msoEh9YdVbXQNYsR84zy
Request ID: 1656030190445296000
Digest: b80e18981b06cb2265c2a42ceff9c43c3c5655ee1e589dc8b26a941013d31f

Transaction
Type: CRED_DEF
Reference: 61
Signature type: CL
Tag: doctorCredential
Attributes:
  • birthday
  • birthmonth
  • birthplace
  • birthyear
  • firstname
  • identifiernumber
  • lastname
  • master_secret
    
```

(d) CRED\_DEF Transaction

Figure 5.17. Ledger transactions



## 5.5.2 Experimental Analysis

Our initial idea was to create a front-end tool that uses an API to interact with ACA-Py for maintaining and querying lists of schema, credentials, connections, etc.

### 5.5.2.1 Performance evaluation

In our study, we focus on evaluating the performance of DSMAC using two experiments:

- *Experiment 1:* Evaluate the performance of the Role-based Decentralized Access Control (RDAC) model using the number of submitted and executed transactions, as well as the number of users.
- *Experiment 2:* Evaluate the performance of the Attributes-based Decentralized Access Control (ADAC) model using DID Document.

Therefore, we show the performance of DSMAC in terms of submitting and executing time which means how fast different Access Control (AC) actions can be performed. The execution time is the most important key parameter for our architectural model. Also, the performance of the DSMAC scheme is focused on the transaction throughput and transaction latency for both experiments. Throughput is described as the number of successful transactions per second (tps). Latency is specified as the average time interval between the initialization of the transaction and the actual execution of the transaction. Moreover, to reduce the cost of cryptographic computations and maintain data confidentiality, the computations are securely outsourced to a more powerful device like a mobile phone. Finally, we examine transaction scalability and sustainability.

5.5.2.2 Results and discussion

The evaluation process was based on the performance assessment of decentralized access control using smart contracts and the SSI system.

- **Transactions time** We evaluate the Access Control policy assignment time in both experiments. Figure 5.18 shows how Access Control policy assignment time varies according to several transactions in the RDAC. We can notice that when the number of transactions increases, the AC policy assignment time is increased. The average time to assign an AC policy using submitted and executed transactions is around 68 ms.

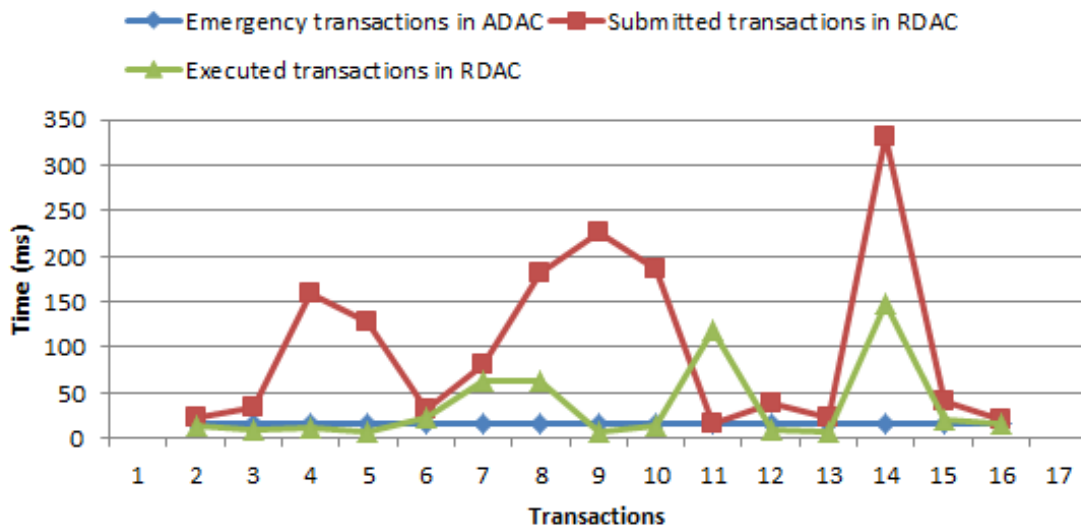


Figure 5.18. Transaction time comparison of RDAC and ADAC models

However, the time is almost unchanged in the ADAC experiment and the average time is around 16 ms. The results show that the ADAC model takes less Access Control assignment time. Thus, in the emergency case, the ADAC model is the best choice.

- **Transaction throughput** The DSMAC system may generate a large volume of access request transactions in RDAC experiments that need to be processed and handled. We measured the transaction throughput while increasing the number

of users, then we compared the transaction throughput of RDAC and ADAC experiments.

Thus, to analyze the throughput, we evaluated the number of access request transactions (txs) that can be executed per second for both experiments, as shown in Figure 5.19. The throughput of a user  $u$  during a time between  $T_i$  and  $T_j$  can be calculated using (eq. 5.6).

$$Throughput_u = \frac{count(tx\ in\ (T_i, T_j))}{T_j - T_i} (txs/s) \quad (5.6)$$

To calculate the average throughput, we can use (eq. 5.7).

$$Throughput = \frac{\sum_u (throughput_u)}{N} (txs/s) \quad (5.7)$$

Initially, the throughput on both models is almost equal. Since the ADAC scheme did not have the credentials verification step and queries are not updating the ledger status, compared to the RDAC model, ADAC has a high throughput. In addition, there is an important increase observed in the throughput of the ADAC model when the number of users is increased, as shown in Figure 5.19. Likewise, the query transaction throughput of ADAC is higher than RDAC.

- **Transaction latency** The latency measures the time of a transaction from submission by the user until it is processed and written into the ledger. Latency values for each experiment are shown in Figure 5.20 using 500 users. It is noticed that there is continuous growth in the average latency as the number of users is increasing for both experiments. The average latency of the ADAC model is lower than the RDAC model. Moreover, It is important to mention that the higher level of security, the lower the latency.
- **Cryptographic computations** In this section, we analyzed the encryption time, CPU consumption, and memory utilization on the mobile device. The study conducted several experiments to encrypt different medical data of different

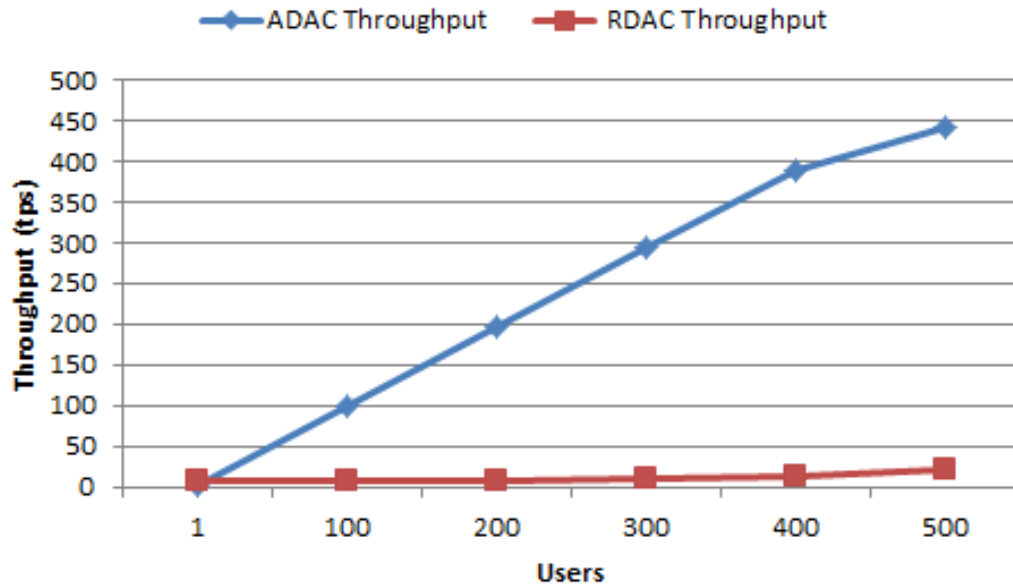


Figure 5.19. Transaction throughput of RDAC and ADAC models.

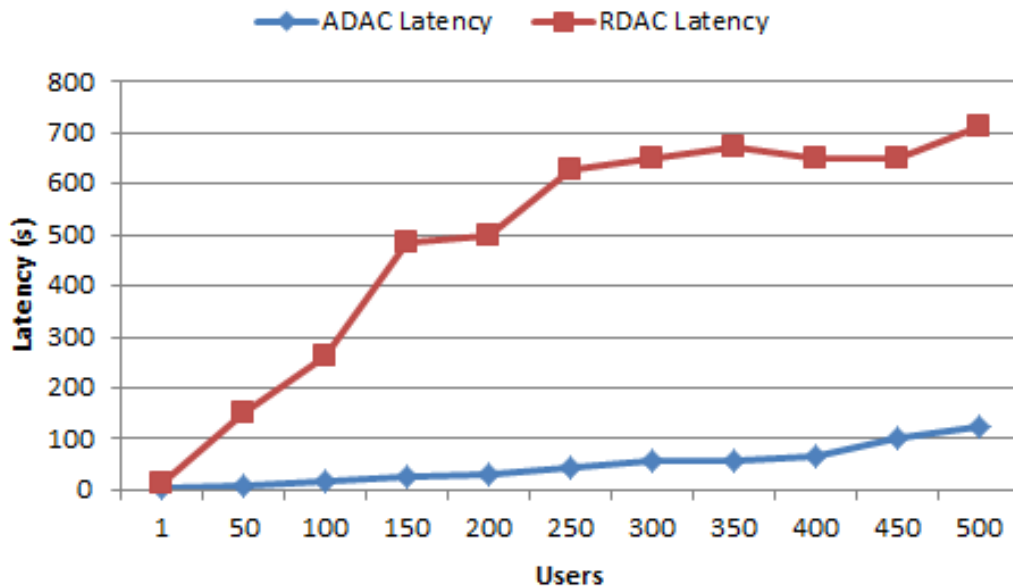
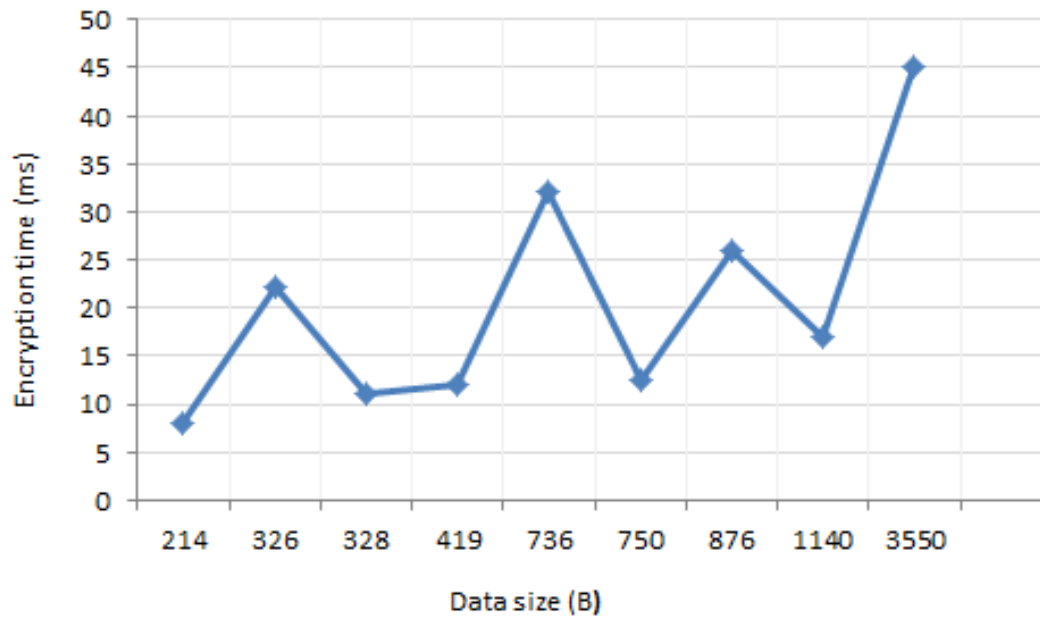


Figure 5.20. Transaction latency of RDAC and ADAC models

sizes, as illustrated in Figure 5.21. The encryption process starts by permitting the DO to select data, then the mobile application encrypts the data using the Zero Knowledge Encryption algorithm.

Figure 5.22 shows the current usage of CPU and memory. We noticed that when the data size is increased, the CPU utilization increases gradually because when



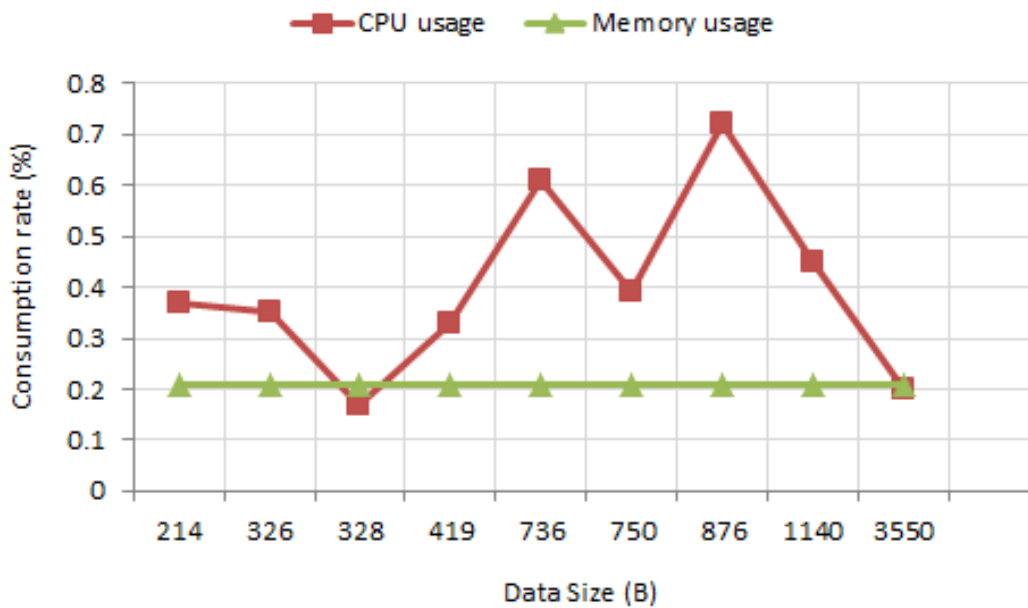
**Figure 5.21.** Time while performing data encryption

**Table 5.2.** Encryption time

| The method proposed by Yonata et al. |                       | The method proposed in DSMAC |                      |
|--------------------------------------|-----------------------|------------------------------|----------------------|
| Data size(KB)                        | Time to encrypt (sec) | Data size (KB)               | Time to encrypt (ms) |
| 25.44                                | 4                     | 0.87                         | 26                   |
| 200                                  | 5                     | 3.55                         | 45                   |
| 600                                  | 7                     | 1.14                         | 17                   |

we increase the number of files, more transactions are sent and this means more CPU computations are recorded. Whereas, memory utilization remains almost constant. Table 5.2 displays a comparison between the encryption time taken by the DSMAC model and other encryption schemes. As a general observation, DSMAC consumed fewer resources compared to other systems.

- **Scalability** In the DSMAC model, scalability is analyzed through transaction throughput and transaction latency. If the throughput remains constant or increases with the increase in the number of users, then the framework is scalable. In another way, if the latency remains constant, then it is also considered a scalable framework that can maintain stable latency in a large-scale environment.
- **Sustainability** DSMAC framework brings a sustainable decentralized access control model without the involvement of the central entity based on sustainable



**Figure 5.22.** CPU and memory usage while performing data encryption

DID solutions. The DID technique can increase patients' ability to contribute to building long-term sustainability. Thus, achieving sustainability in health care is critical for improving the identification of health system functions. Enhancing sustainability, through DID assignment, and managing resources efficiently, will deliver better outcomes for patients, and provide economic benefits.

## 5.6 Security and privacy analysis

In this section, we present the security and privacy analysis after explaining the process of the DSMAC framework. The main goal of an attacker is to gain authorization to access health data. Thus, we present the theoretical analysis of how DSMAC can efficiently resist the attacks proposed in the adversary model.

### 5.6.1 Comparison of security properties

Table 5.3 compares the security properties of the DSMAC framework with:

**Table 5.3.** Comparison between related works and our DSMAC model

| Models                        | Bc-based-AC | SSI-based-AC | Access control methods   |   |                      | Features    |                |              |                |
|-------------------------------|-------------|--------------|--------------------------|---|----------------------|-------------|----------------|--------------|----------------|
|                               |             |              | Identification           | Authentication                          | Authorization        | Scalability | Sustainability | Data privacy | Emergency case |
| Yue et al., 2016              | ✓           | X            | -                        | -                                       | -                    | ✓           | X              | ✓            | X              |
| BBDS (Xia et al., 2017)       | ✓           | X            | Cryptographic keys       | Encryption-digital signatures           | -                    | ✓           | X              | ✓            | X              |
| Ancile (Dagher et al., 2018)  | ✓           | X            | IDs                      | -                                       | Smart contract       | ✓           | X              | ✓            | X              |
| EACMS (Rajput et al., 2019)   | ✓           | X            | Patient ID               | -                                       | Chaincode            | X           | X              | x            | ✓              |
| Healthchain (Xu et al., 2019) | ✓           | X            | Userchain address        | Public key Cryptography                 | -                    | ✓           | X              | ✓            | X              |
| Lagutin et al., 2019          | X           | ✓            | DID                      | Authorization Server                    | Authorization Server | ✓           | X              | ✓            | X              |
| Jung, 2020                    | X           | ✓            | DID                      | Decentralized Public Key Infrastructure | DID and DPKI         | ✓           | X              | X            | X              |
| Kumar et al. (2021)           | ✓           | X            | Secure proof of identity | -                                       | Smart contract       | ✓           | X              | ✓            | X              |
| Madine et al., 2020           | ✓           | X            | -                        | Ethereum address                        | Re-encryption key    | ✓           | X              | ✓            | X              |
| SSIBAC (Belchior et al. 2020) | ✓           | ✓            | DID                      | Decentralized authentication            | Smart contract       | ✓           | X              | ✓            | X              |
| Kim et al., 2021              | ✓           | ✓            | DID                      | DID + VC                                | -                    | X           | X              | ✓            | X              |
| <b>Our DSMAC model</b>        | ✓           | ✓            | DID                      | Public key +DID                         | Smart contract DDO   | ✓           | ✓              | ✓            | ✓              |

- Blockchain-based access control schemes:** Yue et al. (2016), Kumar and Tripathi (2021), Dagher et al. (2018), Xu et al. (2019), Xia et al. (2017a), Rajput et al. (2019), Madine et al. (2020).
- SSI based access control schemes:** Belchior et al. (2020), Lagutin et al. (2019), Jung (2021).

From the table, we notice that almost all the schemes have the properties of scalability and data privacy, which are critical security objectives in health record-sharing systems. Notably, only DSMAC and Rajput schemes (Rajput et al.,

2019) take into consideration the emergency case and no research dealt with the property of sustainability, except the DSMAC model.

### **5.6.2 Privacy protection**

Several privacy-preserving techniques have been employed to achieve privacy in DSMAC. Thus, the encryption of all medical data stored in the F2C prevents the users and other malicious parties to learn the content of the medical data, achieving both patient privacy and health data confidentiality. In addition, DIDs and VCs managed by the digital wallet can be used as a preliminary step to promote privacy-preserving medical data. DSMAC also achieves privacy preservation by anonymity by utilizing the ZKP protocol to ensure that malicious parties cannot deduce the data owners. During this protocol, specific aspects of a VC can be encapsulated through a ZKP method which allows the owner to prove an aspect of his identity without requiring any specific information about that aspect to be disclosed to other parties. Anonymization can be performed by the patient and it is required when the identifying information needs to be hidden from certain parties (Sookhak et al., 2021) such as researchers, pharmacists, etc. However, physicians, nurses, and emergency medical technicians should be able to view such information to carry out proper treatment.

### **5.6.3 Access Control protection**

In the DSMAC system, the honest but curious model is adopted. The end-users are honest since all of them need access control policies to perform their assigned tasks. However, some of them are curious since they continuously can view and store patients' information. In addition, the RDAC scheme is used to address the issue of who can access medical records, and additional schemes are added for emergency cases such as an ADAC approach. This approach is more precise in restricting access based on the DID document and blockchain.



Therefore, the advantage of eliminating the trusted third party makes the decentralized access policy scheme suitable for user privacy-oriented scenarios. The immutability and integrity features of blockchain make it impossible for any user to manipulate, modify, or falsify access control policies stored on the blockchain. Moreover, each block of information contains a hash for itself and for the previous block to verify that the access control policies are not modified illegally. Also, DSMAC is based on smart contracts (Sookhak et al., 2021) and SSI technologies which improve the security of the system such as authorization and privacy-preserving data.

#### **5.6.4 Attacks analysis**

Our decentralized access control system plays a vital role to protect health data against unauthorized access. Therefore, the attacker could not intercept, update or retrieve the medical data with unauthorized access. In this section, we present the resistance model of some attacks threatening the access process such as replay attacks, spoofing attacks, and credential-stuffing attacks.

##### **5.6.4.1 Replay attack resistant**

DSMAC is based on blockchain to provide better access control mechanisms. Every transaction is embedded with nonce value and timestamps (Lippi and others J, 2017). Even each block is linked with the previous hash; hence all communications are chained together. In this way, no one can alter its contents making it impossible for replay attacks to occur. We note that blockchain defends against transaction replay which will provide the system with a protection model against replay attacks.

Furthermore, to acquire authorization, the attacker can try to reply to messages using the signature. However, he will not be successful, since each user has to use a private key and DID to compute the signature. Thus, the adversary is unable to obtain any messages from the user. Therefore, the proposed protocol can resist replay attacks.

#### **5.6.4.2 Spoofing attack resistant**

Spoofing refers to the ability to steal identity information. During this attack, a malicious user presents himself to the system as an authorized user. We have considered the case where an attacker spoofs a user's DID to gain access to medical data. Furthermore, he may change the identity of the data owner. To prevent such attacks, the DSMAC scheme is integrated with a mechanism that allows each user to create a unique DID based on his private key. In addition, we have employed two security primitives to protect against spoofing attacks: (i) the use of the ZKP protocol implies that viewing any transferred data does not reveal any useful information about the user, so only legitimate users whose access has been allowed can use the medical data; (ii) blockchain that holds the access control policies with the hashes generated in every block (van der Merwe et al., 2018). Thus, blockchain with decentralized access control policies maintains reliable and consistent data. Since an attacker cannot inject the wrong DID or address. Also, our proposal is resistant to spoofing attacks because users' DIDs are verified through a ZKP.

#### **5.6.4.3 Credential-stuffing attack resistant**

This attack is the injection of stolen credentials (username and password pairs) to gain unauthorized access to user accounts. In the DSMAC framework, to protect against this attack, each user must authenticate with something he knows such as DID, in addition to something he has such as a mobile phone which plays the role of a digital wallet. The digital wallet contains the DID, private key as well as the VCs of the user, and each user gets a public key which is stored in the blockchain. In this way, the attacker will not be able to provide a physical authentication method. This makes it harder for the attacker, which makes the credential-stuffing attack not possible.

## 5.7 Summary

In this chapter, we presented DSMAC, a decentralized access control system for health data based on the combination of blockchain, RBAC, ABAC, DIDs, and VC. The framework is implemented in a decentralized way to share medical records and preserve security and privacy using smart contracts and self-sovereign identity (SSI) technologies. The choice of the SSI model allows users to own and manage their identities. This makes our framework more suitable for high privacy requirements. DSMAC is based on different contributions aimed to provide benefits in the areas of privacy/security, scalability, and sustainability in the medical environment. Likewise, we compared DSMAC with some typical access control models and implemented a prototype of the proposed framework in regular and emergency cases. The results of the performance evaluation demonstrate that the proposed approach is highly scalable and efficient in terms of submission and execution time, throughput, cryptographic computations, and latency.



---

## General Conclusion

The use of technology had enhanced enormously the lifestyle of patients by facilitating many difficulties and solving a lot of intractable problems. The Internet of Medical Things (IoMT) is one of these popular technologies, it is widely adopted and it can collect medical information in real-time and realize the ubiquitous connection between medical things and patients. Such adoption requires choosing suitable architecture for data storage, data processing, and data analytics like F2C computing. However, some of these technologies had introduced other drawbacks, such as the lack of privacy as well as the different attacks and threats.

Thus, in this thesis, the theoretical aims are based on a detailed analysis of the security requirements, privacy issues, threats, and available solutions in the F2C-based IoMT. Moreover, the technical goal is to create revolutionary systems for privacy-preserving medical data utilizing new technologies like F2C computing, blockchain, and the Self-Sovereign Identity (SSI) concept.

To provide a deep study of the proposed approaches, we have proposed two primary contributions in this thesis.

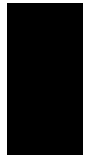
The first one presented a secure health monitoring system based on fog to cloud computing. We suggested a HIPAA-compliant system based on fog-to-cloud (F2C) computing that enables the security and privacy-preserving of medical data. The F2C infrastructure is utilized to enable real-time diagnosis of geriatric patients and enhance

security concerns while combining the advantages of cloud and fog computing, such as permanent storage, decreased compute load and data transmission latency, and enhancing the security challenges.

The second contribution proposed a Decentralized Self-Management of data Access Control system, called the DSMAC system. The blockchain-based Self-Sovereign Identity (SSI) model for privacy-preserving medical data is used by the DSMAC model to protect the privacy of medical data. It also provides patients with mechanisms to maintain control over their personal information and allows them to self-grant access rights to their medical data. DSMAC leverages smart contracts to conduct Role-based Access Control policies and adopts the implementation of decentralized identifiers and verifiable credentials to describe advanced access control techniques for emergency cases.

In the future, to address the privacy issues in the F2C-IoMT domain, we intend on exploiting other aspects than those mentioned in the current thesis. In this section, We outline two future projects:

1. *Artificial Intelligence (AI) for IoMT* : We are interested in exploiting the Artificial Intelligence (AI) concept to identify, track and monitor patients through multiple devices, including when they are at work, at home, or out in public. The objectives and aims of applying AI technology in the IoMT domain are improving the functionality and security challenges, detection accuracy, and decision-making ability of IoMT devices.
2. *Differential privacy (DP)*: Also, we intend to incorporate the use of differential privacy (DP) in our future research to enhance the patient's privacy. Therefore, differential privacy has gained a lot of attention in recent years as a general model for the protection of personal data. It has also been proposed as an appropriate model for protecting health data. Our objective is to apply DP technology in the IoMT domain-based F2C to protect the individual's privacy.



---

# Publications

Received 22 August 2022, accepted 13 September 2022, date of publication 19 September 2022,  
date of current version 29 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3207803


**RESEARCH ARTICLE**

# DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data

HAFIDA SAIDI<sup>1</sup>, NABILA LABRAOUI<sup>2</sup>, ADO ADAMOU ABBA ARI<sup>3,4</sup>,  
LEANDROS A. MAGLARAS<sup>5</sup>, (Senior Member, IEEE),  
AND JOEL HERVE MBOUSSAM EMATI<sup>4</sup>

<sup>1</sup>STIC Laboratory, University of Abou Bekr Belkaid, Chetouane, Tlemcen 13000, Algeria

<sup>2</sup>LRI Laboratory, University of Abou Bekr Belkaid, Chetouane, Tlemcen 13000, Algeria

<sup>3</sup>DAVID Laboratory, Université Paris-Saclay, University of Versailles Saint-Quentin-en-Yvelines, 78000 Versailles, France

<sup>4</sup>Department of Computer Science, University of Maroua, Maroua, Cameroon

<sup>5</sup>School of Computer Science and Informatics, De Montfort University, LE1 9BH Leicester, U.K.

Corresponding authors: Hafida Saidi (hafida.saidi@univ-tlemcen.dz) and Leandros A. Maglaras (leandros.maglaras@dmu.ac.uk)

**ABSTRACT** In recent years, the interest in using wireless communication technologies and mobile devices in the healthcare environment has increased. However, despite increased attention to the security of electronic health records, patient privacy is still at risk for data breaches. Thus, it is quite a challenge to involve an access control system especially if the patient's medical data are accessible by users who have diverse privileges in different situations. Blockchain is a new technology that can be adopted for decentralized access control management issues. Nevertheless, different scalability, security, and privacy challenges affect this technology. To address these issues, we suggest a novel Decentralized Self-Management of data Access Control (DSMAC) system using a blockchain-based Self-Sovereign Identity (SSI) model for privacy-preserving medical data, empowering patients with mechanisms to preserve control over their personal information and allowing them to self-grant access rights to their medical data. DSMAC leverages smart contracts to conduct Role-based Access Control policies and adopts the implementation of decentralized identifiers and verifiable credentials to describe advanced access control techniques for emergency cases. Finally, by evaluating performance and comparing analyses with other schemes, DSMAC can satisfy the privacy requirements of medical systems in terms of privacy, scalability, and sustainability, and offers a new approach for emergency cases.

**INDEX TERMS** Blockchain, data privacy, decentralized access control, decentralized identifier (DID), IoMT sensors, self sovereign identity (SSI), smart contract, verifiable credential (VC).

## I. INTRODUCTION

Over the past few decades, the world has become more connected with the wide adoption of networking and wireless communication technologies, and mobile devices. This evolution lets healthcare organizations and researchers think about benefiting from these technologies to solve the current challenges that the medical technologies are facing, by transforming unsustainable healthcare systems into sustainable ones [1], [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaojie Su<sup>6</sup>.

Patients are increasingly exploiting mobile devices for their medical needs to promote the availability of their medical data and to help avoid repeated examinations. However, the sharing and privacy of medical data represent major technological, legal, and operational challenges [3]. Likewise, the identification of the patient is of critical importance for performing transactions with different healthcare organizations [4]. But by using different identifiers, patients find themselves having to maintain or memorize many combinations of accounts, and they may get interoperability issues, identity loss/theft, and privacy issues. To improve the user identity model, we are considering the concept of

---

## A secure health monitoring system based on fog to cloud computing

---

Hafida Saidi\*

STIC Lab,  
University of Abou Bekr Belkaid,  
Chetouane Tlemcen 13000, Algeria  
Email: hafida.saidi@univ-tlemcen.dz  
\*Corresponding author

Nabila Labraoui

LRI Lab,  
University of Abou Bekr Belkaid,  
Tlemcen 13000, Algeria  
Email: Nabila.labraoui@univ-tlemcen.dz

Ado Adamou Abba Ari

DAVID Lab,  
Université Paris-Saclay,  
University of Versailles Saint-Quentin-en-Yvelines,  
45 Avenue des États-Unis, 78035 Versailles Cedex, France  
and  
Department of Computer Science,  
University of Maroua,  
P.O. Box 814, Maroua, Cameroon  
Email: ado-adamou.abba-ari@uvsq.fr

**Abstract:** Nowadays, the elderly can receive care in their home and enable physicians to follow their diseases in real-time. However, these technologies suffer from several issues like security and privacy-preserving data challenges. In this paper, we proposed a HIPAA-compliant framework that enables security and privacy-preserving medical data based on fog-to-cloud (F2C) computing. Our aims are to define a system that solves the privacy and security issues with remote elderly monitoring. The F2C infrastructure is used to provide better security of medical data and allow a real-time diagnosis of the elderly. Furthermore, F2C combines the benefits of cloud and fog computing such as providing permanent storage, reducing computation load and data transmission delay, and enhancing the security challenges. Simulation results suggest that F2C technology delivers better performance in terms of latency, cost, and energy consumption.

**Keywords:** elderly healthcare; wearable sensors; fog to cloud computing; AES-ECC encryption; internet of medical things; IoMT.



# Remote health monitoring system of elderly based on Fog to Cloud (F2C) computing

Hafida Saidi  
*STIC Lab*  
*University of Tlemcen*  
 Tlemcen 13000, Algeria  
 hafida.saidi@univ-tlemcen.dz

Djelloul Bouida  
*Faculty of Science*  
*University of Tlemcen*  
 Tlemcen 13000, Algeria  
 djelloul.bouida@univ.tlemcen.dz

Nabila Labraoui  
*STIC Lab*  
*University of Tlemcen*  
 Tlemcen 13000, Algeria  
 nabila.labraoui@univ-tlemcen.dz

Ado Adamou Abba Ari  
*LI-PaRAD Lab,*  
*University of Versailles*  
 Saint-Quentin-en-Yvelines, France  
*LaRI Lab,*  
*University of Maroua,*  
 Maroua Cameroon  
 adoadamou.abbaari@gmail.com

**Abstract-** The majority of older persons are challenged by chronic illnesses, so more innovations are needed for geriatric care. Therefore, technological and modern techniques have been adopted to improve the elderly's health. Different computing solutions have been deployed to store and process the health data such as cloud computing which provides powerful computing resources. However, connecting different kind of things directly to the cloud is inefficient. Fortunately, fog computing has emerged as a new computing solution to complement cloud, it allows computation and data storage closer to the IoT devices. However, managing health data stored in fog computing presents a major issue. It is necessary to consider the importance of performance, availability, storage, and privacy of data in fog computing. In this paper, we propose architecture based on Fog to Cloud computing which is a novel solution and innovative approach that contribute to enhance the synergy between the cloud and fog computing to facilitate the management of elderly health data. To analyze the performance of our model in Fog to Cloud environment, FogWorkflowSim toolkit has been used.

**Keywords -** Elderly people, Cloud computing, Fog computing, F2C computing, Medical Data.

## I. INTRODUCTION

Aging is a natural process in a person's life. The majority of older persons are challenged by chronic illnesses and they require continuous monitoring, especially elderly persons living alone. However, the rapid growth of information and communication technologies, such as Internet of Things (IoT), cloud computing, wireless sensors and mobile phones [1, 2] can enhance the development of a monitoring systems to detect elderly people changes and to intervene in real time [3]. Thus, these evolutions place the privacy of the older people at high risk situation and older adults do not have sufficient knowledge to protect themselves [4], their healthcare data can be lost, corrupted, destroyed or even diverted. Fortunately, the emergence of a new and modern computing model referred to as Fog to Cloud (F2C) computing promises to address the security and privacy issues [5]. Our motivation in

this work is the remote monitoring of elderly, and design a method for solving the privacy protection issues for healthcare data based on F2C computing scheme.

In this paper, we focus on extending elderly home care in the safest possible conditions by preventing the risks of people living alone.

The rest of the paper is structured as follows: in section 2 related work is reviewed. Section 3 introduces different computing models. In section 4, we describe our proposed approach and its architecture. Section 5 gives the results of performance evaluation. Finally, we draw conclusion and future work in section 6.

## II. RELATED WORK

Data management in smart hospitals can be based on two different views: centralized and distributed. Data management architectures in smart hospitals rely usually on centralized cloud computing models. The main advantages of cloud computing are its unlimited computing capacity, cost efficiency and the elasticity [6]. Furthermore, transferring all data and resources to the cloud poses several issues, such as high communication latencies, network congestion, and also increases the risks for failures, privacy and security vulnerabilities [7]. Cloud computing has been widely used to store and process the medical data [8]. However, cloud based solutions can cause huge problems in health application, which can create failures or loss of data. In ESPAC [30], patient data will be sent to the hospital server, and then it will be stored on the cloud. However, this scheme has a limited scalability issue, and no data storage or data access are possible on the cloud if the hospital server is inaccessible. A platform for secure monitoring and sharing of health data in the cloud was proposed in [31]. It allows secure sharing of medical data. However, users' requests must first pass through a trusted party before they access on the cloud where

# Real-time Aging Friendly fall detection system

Hafida Saidi  
 STIC Lab  
 University of Tlemcen  
 Tlemcen, Algeria  
 hafida.saidi@univ-tlemcen.dz

Nabila Labraoui  
 STIC Lab  
 University of Tlemcen  
 Tlemcen, Algeria  
 nabila.labraoui@univ-tlemcen.dz

Ado Adamou Abba Ari  
 LI-PaRAD Lab, University of  
 Versailles Saint-Quentin-en-  
 Yvelines, France  
 And LaRI Lab, University of  
 Maroua, Cameroon  
 adoadamou.abbaari@gmail.com

Ikram Smahi  
 Faculty of Science  
 University of Tlemcen  
 Tlemcen, Algeria  
 ikramsemahi@gmail.com

Bouchera Ramdane Mamcha  
 Faculty of Science  
 University of Tlemcen  
 Tlemcen, Algeria  
 fatima13.abo@gmail.com

**Abstract** - The fall is a crucial issue for elderly people. With the strong growth of information and communication technologies and the development of light and low-cost wearable technology, elderly fall detection has gained much attention. These technologies can help the elderly get timely assistance to reduce further injury. In this paper, we propose to develop a real-time aging friendly fall detection system based on acceleration and angular velocity values produced by the accelerometer and gyroscope sensors of the mobile device. We describe an effective and simple threshold-based solution to implement a real-time method to monitor the elderly and detect falls using a mobile phone. In case of a fall, our system will transmit an alert with location information to the contacts list via a notification. Thus, medical attention can be provided with minimal delay. The system was tested by volunteers and achieved high sensitivity, specificity and accuracy.

**Index Terms** - Fall detection, Accelerometer, gyroscope, elderly people, mobile phones.

## I. INTRODUCTION

In recent years, the world is moving rapidly towards the new era of the Internet-of-Things (IoT). Thus, IoT has acquired much attention from researchers and technology giants around the world [1,2,3]. It is an emerging technology that connects a variety of devices and systems such as sensors, computers and mobile phones. Technological advances have opened the door to the IoT applications with ample opportunities. The best tool that can be used to properly harness the benefits of IoT solutions is the mobile phone. Accessing IoT solutions via mobile applications is inexpensive and offer more flexible platform for transmitting data compared to web applications. E-health is an example of a gerontechnology IoT application that can play a crucial role in revolutionizing the elderly healthcare system.

The majority of the elderly are challenged by chronic and acute illnesses and/or injuries. For this purpose, elderly persons require continuous monitoring. So, more investment is needed for geriatric care. The strong development of the technologies can foster the

creation of monitoring and intervention systems to quickly detect changes of the elderly in real-time and to intervene correctly and on time [4].

One of the major risks incurred by the elderly population is falling. Falls are a serious problem for both families and medical professionals; they represent one of the major causes of death [5]. Thus, fall detection is a critical event requiring a quick and accurate response, especially for the elderly's independent living [5]. This automatic fall detection would help to reduce the arrival time of medical personnel and reduce the risks of the complications. To detect the elderly fall using the mobile phone, accelerometer and gyroscope sensors embedded in a smartphone are used. The placement of the mobile phone at the waist is been thought to be ideal when compared to the wrist and knee [6]. Moreover, Waist attached accelerometers are situated near the body's center of gravity, providing reliable information on user body movements [6]. In this paper, we propose to develop a real-time aging friendly fall detection system based on acceleration values and angular velocity, produced by an accelerometer and gyroscope sensors of the mobile device. We describe an effective and simple threshold-based solution to implement a real-time method to monitor the elderly and detect falls using a mobile phone with a tri-axial accelerometer and gyroscope. The main goal of our paper is to ease the older generation into this world, provide a simple and user-friendly way to alert contacts list during an event. This can be a fast and easy instrument for first aid.

The rest of this paper is organized as follows: in section 2 related work is discussed. Section 3 gives the system model and the basic algorithm of the threshold-based fall detection is introduced. In Section 4, details on the evaluation of the proposed threshold approach and fall detection algorithm are revealed. Finally, we draw conclusions in Section 5.

## II. RELATED WORK

To solve the elderly fall detection problem, the authors proposed to develop an effective fall detection system to support elderly people, especially for those



---

## Bibliography

- Abdullah, A. M. et al. (2017). Advanced encryption standard (aes) algorithm to encrypt and decrypt data, *Cryptography and Network Security* **16**: 1–11.
- Acar, A. et al. (2018). A survey on homomorphic encryption schemes: Theory and implementation, *ACM Computing Surveys (Csur)* **51**(4): 1–35.
- Ahmad, M. et al. (2016). Health fog: a novel framework for health and wellness applications, *The Journal of Supercomputing* **72**(10): 3677–3695.
- Ahmid, M., Kazar, O. and Kahloul, L. (2022). A secure and intelligent real-time health monitoring system for remote cardiac patients., *Int. J. Medical Eng. Informatics* **14**(2): 134–150.
- Airehrour, D., Madanian, S. and Abraham, A. M. (2018). Designing a memory-aid and reminder system for dementia patients and older adults.
- Al Hamid, H. A. et al. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography, *IEEE Access* **5**: 22313–22328.
- Al Omar, A. et al. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment, *Future generation computer systems* **95**: 511–521.

- Al-Zubaidie, M., Zhang, Z. and Zhang, J. (2019). Pax: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system, *International Journal of Environmental Research and Public Health* **16**(9): 1490.
- Allen, C. (2016). The path to self-sovereign identity, *Life with Alacrity* .
- Allison, D. S. et al. (2016). An ontology driven privacy framework for collaborative working environments, *International Journal of Autonomous and Adaptive Communications Systems* **9**(3-4): 243–268.
- Almeida, A. et al. (2017). An iot-aware architecture for collecting and managing data related to elderly behavior, *Wireless Communications and Mobile Computing* **2017**.
- Ari, A. A. A. et al. (2020). Enabling privacy and security in cloud of things: Architecture, applications, security & privacy challenges, *Applied Computing and Informatics* .
- Babaghayou, M., Chaib, N., Lagraa, N., Ferrag, M. A. and Maglaras, L. (2023). A safety-aware location privacy-preserving iov scheme with road congestion-estimation in mobile edge computing, *Sensors* **23**(1): 531.
- Babrahem, A. S. and Monowar, M. M. (2021). Preserving confidentiality and privacy of the patient's ehr using the orbac and aes in cloud environment, *International Journal of Computers and Applications* **43**(1): 50–61.
- Baier, D. et al. (2010). *A Guide to Claims-Based Identity and Access Control: Patterns & Practices*, Microsoft Press.
- Baktyan, A. and Zahary, A. (2018). A review on cloud and fog computing integration for iot: Platforms perspective, *EAI Endorsed Transactions on Internet of Things* **4**(14).
- Banerjee, A. et al. (2022). Blockchain in iot and beyond: Case studies on interoperability and privacy, *Blockchain based Internet of Things*, Springer, pp. 113–138.
- Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights, *Big Data & Society* **6**(2): 2053951719855091.

- Belchior, R. et al. (2020). Ssibac: self-sovereign identity based access control, 2020 *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE, pp. 1935–1943.
- Bhardwaj, K. and Chaudhary, S. (2012). Implementation of elliptic curve cryptography in 'c', *International Journal on Emerging Technologies* 3(2): 38–51.
- Bhushan, K. et al. (2017). Ddos attack defense framework for cloud using fog computing, 2017 *2nd IEEE international conference on recent trends in electronics, information & communication technology (RTEICT)*, IEEE, pp. 534–538.
- Brossard, D., Gebel, G. and Berg, M. (2017). A systematic approach to implementing abac, *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control*, pp. 53–59.
- Burkhart, M. et al. (2010). Sepia: Privacy-preserving aggregation of multi-domain network events and statistics, *19th USENIX Security Symposium (USENIX Security 10)*.
- Capraz, S. and Ozsoy, A. (2021). Personal data protection in blockchain with zero-knowledge proof, *Blockchain Technology and Innovations in Business Processes*, Springer, pp. 109–124.
- Casciaro, S. et al. (2020). A smart pill dispenser to support elderly people in medication adherence, 2020 *5th International Conference on Smart and Sustainable Technologies (SpliTech)*, IEEE, pp. 1–6.
- Cha, S.-C. et al. (2018). Privacy enhancing technologies in the internet of things: Perspectives and challenges, *IEEE Internet of Things Journal* 6(2): 2159–2187.
- Clarke, R. (2006). What's' privacy', *Proc. of the Workshop at the Australian Law Reform Commission*.
- Colombo, P. and Ferrari, E. (2015). Privacy aware access control for big data: A research roadmap, *Big Data Research* 2(4): 145–154.

- Cramer, R., Damgård, I. and Maurer, U. (2000). General secure multi-party computation from any linear secret-sharing scheme, *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 316–334.
- Cruz, J. P., Kaji, Y. and Yanai, N. (2018). Rbac-sc: Role-based access control using smart contract, *Ieee Access* **6**: 12240–12251.
- Dagher, G. G. et al. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, *Sustainable cities and society* **39**: 283–297.
- Djam-douou, M., Ari, A. A. A., Mboussam, H. J. E., Ndam, N. A., Thiare, O., Labraoui, N. and Gueroui, A. M. (2023). A certificate-based pairwise key establishment protocol for iot resource-constrained devices, *Ngatched, T.M.N., Woungang, I., Tapamo, J.R., Viriri, S. (eds) Pan-African Artificial Intelligence and Smart Systems. PAAISS 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Vol. 459, Springer, Cham, pp. 1–16.
- Dolui, K. and Datta, S. K. (2017). Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing, *2017 Global Internet of Things Summit (GloTS)*, IEEE, pp. 1–6.
- Dorri, A. et al. (2017). Blockchain for iot security and privacy: The case study of a smart home, *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, IEEE, pp. 618–623.
- Duan, Y., Canny, J. and Zhan, J. (2010). P4p: Practical Large-Scale Privacy-Preserving distributed computation robust against malicious users, *19th USENIX Security Symposium (USENIX Security 10)*.
- Dwivedi, A. D. et al. (2019). A decentralized privacy-preserving healthcare blockchain for iot, *Sensors* **19**(2): 326.
- Dwork, C. et al. (2006). Calibrating noise to sensitivity in private data analysis, *Theory of cryptography conference*, Springer, pp. 265–284.

- Edwards, B., Hofmeyr, S. and Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches, *Journal of Cybersecurity* **2**(1): 3–14.
- Ehret, A. et al. (2021). Reconfigurable hardware root-of-trust for secure edge processing, *2021 IEEE High Performance Extreme Computing Conference (HPEC)*, IEEE, pp. 1–7.
- Eichler, S. et al. (2017). Effectiveness of an interactive telerehabilitation system with home-based exercise training in patients after total hip or knee replacement: study protocol for a multicenter, superiority, no-blinded randomized controlled trial, *Trials* **18**(1): 1–7.
- ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE transactions on information theory* **31**(4): 469–472.
- Farahani, B. et al. (2018). Towards fog-driven iot ehealth: Promises and challenges of iot in medicine and healthcare, *Future Generation Computer Systems* **78**: 659–676.
- Ferdous, M. S., Ionita, A. and Prinz, W. (2023). Ssi4web: A self-sovereign identity (ssi) framework for the web, *International Congress on Blockchain and Applications*, Springer, pp. 366–379.
- Froelicher, D. et al. (2017). Unlynx: A decentralized system for privacy-conscious data sharing., *Proc. Priv. Enhancing Technol.* **2017**(4): 232–250.
- Gajanayake, R., Iannella, R. and Sahama, T. (2014). Privacy oriented access control for electronic health records, *Electronic Journal of Health Informatics* **8**(2): Article–number.
- Gassmann, H. P. (1981). Oecd guidelines governing the protection of privacy and transborder flows of personal data, *Computer Networks (1976)* **5**(2): 127–141.
- Gill, S. S. et al. (2018). Fog-based smart healthcare as a big data and cloud service for heart patients using iot, *International Conference on Intelligent Data Communication Technologies and Internet of Things*, Springer, pp. 1376–1383.

- Goldwasser, S., Micali, S. and Rackoff, C. (2019). The knowledge complexity of interactive proof-systems, *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pp. 203–225.
- González-Manzano, L. et al. (2016). Pagiot–privacy-preserving aggregation protocol for internet of things, *Journal of Network and Computer Applications* **71**: 59–71.
- Grassi, P. A., Garcia, M. E. and Fenton, J. L. (2017). Draft nist special publication 800-63-3 digital identity guidelines, *National Institute of Standards and Technology, Los Altos, CA*.
- Grassi, P. A. et al. (2016). Draft nist special publication 800-63b digital identity guidelines, *National Institute of Standards and Technology (NIST)* **27**.
- Guan, Z. et al. (2019). Appa: An anonymous and privacy preserving data aggregation scheme for fog-enhanced iot, *Journal of Network and Computer Applications* **125**: 82–92.
- Habib, M. A. et al. (2018). Speeding up the internet of things: Leaiot: A lightweight encryption algorithm toward low-latency communication for the internet of things, *IEEE Consumer Electronics Magazine* **7**(6): 31–37.
- Hafsa, A. et al. (2017). A hardware-software co-designed aes-ecc cryptosystem, *2017 International Conference on Advanced Systems and Electric Technologies (IC\_ASET)*, IEEE, pp. 50–54.
- Hardjono, T. and Smith, N. (2016). Cloud-based commissioning of constrained devices using permissioned blockchains, *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security*, pp. 29–36.
- Harrop, M. (2009). Identity management, *The Cottingham Group, ETSI Security Workshop*.
- Hashemi, S. H. et al. (2016). World of empowered iot users, *2016 IEEE first international conference on internet-of-things design and implementation (IoTDI)*, IEEE, pp. 13–24.



- He, J. et al. (2016). Consensus-based privacy-preserving data aggregation, *arXiv preprint arXiv:1609.06381* .
- Helliar, C. V. et al. (2020). Permissionless and permissioned blockchain diffusion, *International Journal of Information Management* **54**: 102136.
- Hewison, A. and Morrell, K. (2014). Leadership development in the english national health service: A counter narrative to inform policy, *International journal of nursing studies* **51**(4): 677–688.
- HiPAA, H. (2010). Health information privacy, <http://www.hhs.gov/ocr/privacy> **Accessed: November 2022**.
- Hoepman, J.-H. (2014). Privacy design strategies, *IFIP International Information Security Conference*, Springer, pp. 446–459.
- Hu, J., Chen, H.-H. and Hou, T.-W. (2010). A hybrid public key infrastructure solution (hpki) for hipaa privacy/security regulations, *Computer Standards & Interfaces* **32**(5-6): 274–280.
- IEC, I. (n.d.). 29100, 2011, *BS ISO/IEC29100: Information Technology—Security Techniques—Privacy Framework*. Available online: <https://www.iso.org/standard/45123.html> (accessed on 14 November 2019) .
- Isa, I. S. M. et al. (2018). Energy efficiency of fog computing health monitoring applications, *2018 20th International Conference on Transparent Optical Networks (ICTON)*, IEEE, pp. 1–5.
- Jayaraman, P. P. et al. (2017). Privacy preserving internet of things: From privacy techniques to a blueprint architecture and efficient implementation, *Future Generation Computer Systems* **76**: 540–549.
- Jung, E. (2021). A decentralized access control model for iot with did, *IT Convergence and Security*, Springer, pp. 141–148.

- Khader, A. H. A. and Subasri, K. (2020). Fog assisted-iot enabled patient health monitoring, *Adalya J* **9**: 525–530.
- Kim, B. et al. (2021). Attribute-based access control (abac) with decentralized identifier in the blockchain-based energy transaction platform, *2021 International Conference on Information Networking (ICOIN)*, IEEE, pp. 845–848.
- Kocabas, O. and Soyata, T. (2020). Towards privacy-preserving medical cloud computing using homomorphic encryption, *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice*, IGI Global, pp. 93–125.
- Kondova, G. and Erbguth, J. (2020). Self-sovereign identity on public blockchains and the gdpr, *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pp. 342–345.
- Korzun, D. G. et al. (2015). Digital assistance services for emergency situations in personalized mobile healthcare: Smart space based approach, *2015 International Conference on Biomedical Engineering and Computational Technologies (SIBIRCON)*, IEEE, pp. 62–67.
- Kotronis, C. et al. (2019). Evaluating internet of medical things (iomt)-based systems from a human-centric perspective, *Internet of Things* **8**: 100125.
- Kravets, R., Tuncay, G. S. and Sundaram, H. (2015). For your eyes only, *Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services*, pp. 28–35.
- Kumar, R. and Tripathi, R. (2021). Scalable and secure access control policy for healthcare system using blockchain and enhanced bell-lapadula model, *Journal of Ambient Intelligence and Humanized Computing* **12**(2): 2321–2338.
- Kute, V. B., Paradhi, P. and Bamnote, G. (2009). A software comparison of rsa and ecc, *Int. J. Comput. Sci. Appl* **2**(1): 43–59.
- Lagutin, D. et al. (2019). Enabling decentralised identifiers and verifiable credentials for constrained iot devices using oauth-based delegation, *Proceedings of the Workshop*

- on Decentralized IoT Systems and Security (DISS 2019), in Conjunction with the NDSS Symposium, San Diego, CA, USA, Vol. 24.*
- Li, M. et al. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings, *International conference on security and privacy in communication systems*, Springer, pp. 89–106.
- Li, M. et al. (2018). Crowdbc: A blockchain-based decentralized framework for crowdsourcing, *IEEE Transactions on Parallel and Distributed Systems* **30**(6): 1251–1266.
- Li, N., Li, T. and Venkatasubramanian, S. (2006).  $t$ -closeness: Privacy beyond  $k$ -anonymity and  $l$ -diversity, *2007 IEEE 23rd international conference on data engineering*, IEEE, pp. 106–115.
- Liang, K., Susilo, W. and Liu, J. K. (2015). Privacy-preserving ciphertext multi-sharing control for big data storage, *IEEE transactions on information forensics and security* **10**(8): 1578–1589.
- Liang, X. et al. (2017). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, IEEE, pp. 468–477.
- Lim, S. Y. et al. (2022). Trust models for blockchain-based self-sovereign identity management: A survey and research directions, *Advances in Blockchain Technology for Cyber Physical Systems* pp. 277–302.
- Lin, C. et al. (2016). Differential privacy preserving in big data analytics for connected health, *Journal of medical systems* **40**(4): 1–9.
- Lippi, G. and others J (2017). Managing the patient identification crisis in healthcare and laboratory medicine, *Clinical biochemistry* **50**(10-11): 562–567.

- Liu, A. et al. (2019a). Differential privacy for eye-tracking data, *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, pp. 1–10.
- Liu, T. et al. (2021). Efficient decentralized access control for secure data sharing in cloud computing, *Concurrency and Computation: Practice and Experience* p. e6383.
- Liu, X. et al. (2019b). Fogworkflowsim: An automated simulation toolkit for workflow performance evaluation in fog computing, *2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, IEEE, pp. 1114–1117.
- Loza-Matovelle, D. et al. (2019). An architecture for the integration of robots and sensors for the care of the elderly in an ambient assisted living environment, *Robotics* 8(3): 76.
- Lu, R. et al. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot, *IEEE access* 5: 3302–3312.
- Machanavajjhala, A. et al. (2007). l-diversity: Privacy beyond k-anonymity, *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1(1): 3–es.
- Madine, M. M. et al. (2020). Blockchain for giving patients control over their medical records, *IEEE Access* 8: 193102–193115.
- Madiyal, V. (2022). Internet of medical things (iomt) and its impact on healthcare, <https://www.linkedin.com/pulse/internet-medical-things-iomt-its-impact-healthcare-varun-madiyal> **Accessd: November 2022.**
- Mahalle, P. N. and Shinde, G. R. (2021). Oauth-based authorization and delegation in smart home for the elderly using decentralized identifiers and verifiable credentials, *Security issues and privacy threats in smart ubiquitous computing*, Springer, pp. 95–109.
- Mahalle, P. N., Shinde, G. and Shafi, P. M. (2020). Rethinking decentralised identifiers and verifiable credentials for the internet of things, *Internet of things, smart computing and technology: A roadmap ahead*, Springer, pp. 361–374.

- Malik, M. and Patel, T. (2016). Database security-attacks and control methods, *International Journal of Information* **6**(1/2): 175–183.
- Manocha, A. and Singh, R. (2022). A novel edge analytics assisted motor movement recognition framework using multi-stage convo-gru model, *Mobile Networks and Applications* **27**(2): 657–676.
- Manocha, A., Singh, R. and Bhatia, M. (2020). Cognitive intelligence assisted fog-cloud architecture for generalized anxiety disorder (gad) prediction, *Journal of medical systems* **44**(1): 1–20.
- Manoj, T., Makkithaya, K. and Narendra, V. (2022). A blockchain based decentralized identifiers for entity authentication in electronic health records, *Cogent Engineering* **9**(1): 2035134.
- Masip-Bruin, X. et al. (2016a). Fog-to-cloud computing (f2c): The key technology enabler for dependable e-health services deployment, *2016 Mediterranean ad hoc networking workshop (Med-Hoc-Net)*, IEEE, pp. 1–5.
- Masip-Bruin, X. et al. (2016b). Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems, *IEEE Wireless Communications* **23**(5): 120–128.
- Matsui, K. and Choi, H. (2017). Temperature management system to prevent heat shock in households for elderly people, *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIIC/ATC/CBDCCom/IOP/SCI)*, IEEE, pp. 1–6.
- Mehmood, A. et al. (2018). Anonymous authentication scheme for smart cloud based healthcare applications, *IEEE access* **6**: 33552–33567.
- Mendonca, S. N. (2018). Data security in cloud using aes, *Int. J. Eng. Res. Technol* **7**.

- Mivule, K. (2013). Utilizing noise addition for data privacy, an overview, *arXiv preprint arXiv:1309.3958* .
- Mohamed, N. et al. (2021). Applications of integrated iot-fog-cloud systems to smart cities: A survey, *Electronics* **10**(23): 2918.
- Mohandas, A. (2014). Privacy preserving content disclosure for enabling sharing of electronic health records in cloud computing, *Proceedings of the 7th ACM India computing conference*, pp. 1–7.
- Monteiro, K. et al. (2021). Internet of medical things (iomt) applications in e-health systems context, *Emerging Technologies in Biomedical Engineering and Sustainable TeleMedicine* pp. 1–12.
- Mukherjee, M., Shu, L. and Wang, D. (2018). Survey of fog computing: Fundamental, network applications, and research challenges, *IEEE Communications Surveys & Tutorials* **20**(3): 1826–1857.
- Mutlag, A. A. et al. (2019). Enabling technologies for fog computing in healthcare iot systems, *Future Generation Computer Systems* **90**: 62–78.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, *Decentralized Business Review* p. 21260.
- Narayan, S., Gagné, M. and Safavi-Naini, R. (2010). Privacy preserving ehr system using attribute-based infrastructure, *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, pp. 47–52.
- Nasir, Q. et al. (2018). Performance analysis of hyperledger fabric platforms, *Security and Communication Networks* **2018**.
- Nayyar, A., Puri, V. and Nguyen, N. G. (2019). Biosenhealth 1.0: a novel internet of medical things (iomt)-based patient health monitoring system, *International conference on innovative computing and communications*, Springer, pp. 155–164.

- Ouaddah, A., Abou Elkalam, A. and Ait Ouahman, A. (2016). Fairaccess: a new blockchain-based access control framework for the internet of things, *Security and communication networks* **9**(18): 5943–5964.
- O'Connor, Y. et al. (2017). Privacy by design: informed consent and internet of things for smart health, *Procedia computer science* **113**: 653–658.
- Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes, *International conference on the theory and applications of cryptographic techniques*, Springer, pp. 223–238.
- Patel, A. and Shah, J. (2021). Smart ecosystem to facilitate the elderly in ambient assisted living, *Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*, Springer, pp. 501–510.
- Preukschat, A. and Reed, D. (2021). *Self-sovereign identity*, Manning Publications.
- Qi, C. (2009). A zero-knowledge proof of digital signature scheme based on the elliptic curve cryptosystem, *2009 Third International Symposium on Intelligent Information Technology Application*, Vol. 3, IEEE, pp. 612–615.
- Rajput, A. R. et al. (2019). Eacms: Emergency access control management system for personal health record based on blockchain, *IEEE Access* **7**: 84304–84317.
- Rees-Pullman, S. (2020). Is credential stuffing the new phishing?, *Computer Fraud & Security* **2020**(7): 16–19.
- Regulation, P. (2016). Regulation (eu) 2016/679 of the european parliament and of the council, *Regulation (eu)* **679**: 2016.
- Rezaeibagha, F. and Mu, Y. (2016). Distributed clinical data sharing via dynamic access-control policy transformation, *International journal of medical informatics* **89**: 25–31.
- Sadique, K. M., Rahmani, R. and Johannesson, P. (2020). Identity management in internet of things: A software-defined networking approach, *Proceedings of the*

- 2nd International Conference on Communication, Devices and Computing*, Springer, pp. 495–504.
- Saha, R. et al. (2019). Privacy ensured e-healthcare for fog-enhanced iot based applications, *IEEE Access* **7**: 44536–44543.
- Sahu, D. et al. (2021). The internet of things in geriatric healthcare, *Journal of healthcare engineering* **2021**.
- Saidi, H. et al. (2019). Real-time aging friendly fall detection system, *2019 6th International Conference on Image and Signal Processing and their Applications (ISPA)*, IEEE, pp. 1–6.
- Saidi, H. et al. (2020). Remote health monitoring system of elderly based on fog to cloud (f2c) computing, *2020 international conference on intelligent systems and computer vision (ISCV)*, IEEE, pp. 1–7.
- Salis, A. (2022). H2020 eu mf2c project, <https://www.mf2c-project.eu/press-room/use-cases/index.html> **Accessed: October 2022**.
- Sandhu, R. et al. (2000). The nist model for role-based access control: towards a unified standard, *ACM workshop on Role-based access control*, Vol. 10.
- Saraubon, K., Anurugsa, K. and Kongsakpaibul, A. (2018). A smart system for elderly care using iot and mobile technologies, *Proceedings of the 2018 2nd International Conference on Software and e-Business*, pp. 59–63.
- Seneviratne, S. et al. (2017). A survey of wearable devices and challenges, *IEEE Communications Surveys & Tutorials* **19**(4): 2573–2620.
- Shao, F., Chang, Z. and Zhang, Y. (2010). Aes encryption algorithm based on the high performance computing of gpu, *2010 Second International Conference on Communication Software and Networks*, IEEE, pp. 588–590.



- Shewale, M. A. D. and Sankpal, S. (2020). Iot based smart and secure health care system analysis & data comparison, *International Journal for Research in Applied Science and Engineering Technology* **8**(1): 394–398.
- Silas, S. and Rajsingh, E. B. (2019). A novel patient friendly it enabled framework for selection of desired healthcare provider, *International Journal of Medical Engineering and Informatics* **11**(1): 14–40.
- Sinaeepourfard, A. et al. (2017). Fog-to-cloud (f2c) data management for smart cities, *Proceedings of 2017 Future Technologies Conference (FTC): 29-30 November 2017, Vancouver, Canada*, The Science and Information (SAI) Organization, pp. 162–172.
- Singh, P. K., Pandey, A. K. and Bose, S. (2022). A new grey system approach to forecast closing price of bitcoin, bionic, cardano, dogecoin, ethereum, xrp cryptocurrencies, *Quality & Quantity* pp. 1–18.
- Song, L. et al. (2020). Attribute-based access control using smart contracts for the internet of things, *Procedia computer science* **174**: 231–242.
- Sonnino, A. et al. (2020). Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers, *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, pp. 294–308.
- Sood, S. K. (2012). A combined approach to ensure data security in cloud computing, *Journal of Network and Computer Applications* **35**(6): 1831–1838.
- Sood, S. K. and Mahajan, I. (2018). Iot-fog-based healthcare framework to identify and control hypertension attack, *IEEE Internet of Things Journal* **6**(2): 1920–1927.
- Sookhak, M. et al. (2021). Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues, *Journal of Network and Computer Applications* **178**: 102950.
- Spiekermann, S. and Cranor, L. F. (2008). Engineering privacy, *IEEE Transactions on software engineering* **35**(1): 67–82.

- Sporny, M., Longley, D. and Chadwick, D. (2019). Verifiable credentials data model 1.0, *W3C, W3C Candidate Recommendation, March* .
- Sporny, M. et al. (2022). Decentralized identifiers (dids) v1. 0, 2021.
- Steinbrook, R. (2009). Health care and the american recovery and reinvestment act, *New England Journal of Medicine* **360**(11): 1057–1060.
- Sun, J. et al. (2019). An efficient and scalable framework for processing remotely sensed big data in cloud computing environments, *IEEE Transactions on Geoscience and Remote Sensing* **57**(7): 4294–4308.
- Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* **10**(05): 571–588.
- Taneja, H. et al. (2015). Preserving privacy of patients based on re-identification risk, *Procedia Computer Science* **70**: 448–454.
- Thilakanathan, D. et al. (2014). A platform for secure monitoring and sharing of generic health data in the cloud, *Future Generation Computer Systems* **35**: 102–113.
- Thomas, A. M., Ramaguru, R. and Sethumadhavan, M. (2022). Distributed identity and verifiable claims using ethereum standards, *Inventive Communication and Computational Technologies*, Springer, pp. 621–636.
- Tsai, T.-H. et al. (2020). Technology anxiety and resistance to change behavioral study of a wearable cardiac warming system using an extended tam for older adults, *PloS one* **15**(1): e0227270.
- van der Merwe, J. R. et al. (2018). Classification of spoofing attack types, *2018 European Navigation Conference (ENC)*, IEEE, pp. 91–99.
- Vargheese, R. and Viniotis, Y. (2014). Influencing data availability in iot enabled cloud based e-health in a 30 day readmission context, *10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, IEEE, pp. 475–480.

- Xia, Q. et al. (2017a). Bbds: Blockchain-based data sharing for electronic medical records in cloud environments, *Information* **8**(2): 44.
- Xia, Q. et al. (2017b). Medshare: Trust-less medical data sharing among cloud service providers via blockchain, *IEEE access* **5**: 14757–14767.
- Xu, J., Ota, K. and Dong, M. (2020). Fast deployment of emergency fog service for disaster response, *IEEE Network* **34**(6): 100–105.
- Xu, J. et al. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, *IEEE Internet of Things Journal* **6**(5): 8770–8781.
- Yaga, D. et al. (2019). Blockchain technology overview, *arXiv preprint arXiv:1906.11078* .
- Yang, J.-J., Li, J.-Q. and Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment, *Future Generation computer systems* **43**: 74–86.
- Yang, J. et al. (2022). A proof-of-authority blockchain-based distributed control system for islanded microgrids, *IEEE Transactions on Industrial Informatics* **18**(11): 8287–8297.
- Yang, X. and Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain, *Computers & Security* **99**: 102050.
- Yang, Y. et al. (2019). Privacy-preserving smart iot-based healthcare big data storage and self-adaptive access control system, *Information Sciences* **479**: 567–592.
- Yu, Y., Hu, L. and Chu, J. (2020). A secure authentication and key agreement scheme for iot-based cloud computing environment, *Symmetry* **12**(1): 150.
- Yue, X. et al. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, *Journal of medical systems* **40**(10): 1–8.
- Zhang, K. et al. (2014). Phda: A priority based health data aggregation with privacy preservation for cloud assisted wbans, *Information Sciences* **284**: 130–141.

Zia, M. T., Khan, M. A. and El-Sayed, H. (2020). Application of differential privacy approach in healthcare data—a case study, *2020 14th International Conference on Innovations in Information Technology (IIT)*, IEEE, pp. 35–39.

