SECURE LIGHTWEIGHT CLIENT FOR CLOUD-BASED E-HEALTH MODEL

By

ZHANG XIAOWEI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

November 2023

FSKTM 2023 13

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

SECURE LIGHTWEIGHT CLIENT FOR CLOUD-BASED E-HEALTH MODEL

By

ZHANG XIAOWEI

November 2023

Chairman : Azizol bin Hj Abdullah, PhD
Faculty : Computer Science and Information Technology

A strict requirement for the security and privacy of Electronic Health Records (EHRs) is a primary issue for realizing a secure eHealth system. Based on an investigation of medical modes and a questionnaire survey on 114 medical practitioners of several of China's tertiary hospitals, the medical industry needs such high-security EHRs systems while the EHRs systems currently in use cannot meet requirements. The solution to this bottleneck is proposing a novel model for realizing a secure eHealth system.

In this study, a secure cloud-based electronic health system model (SCBEH) is proposed. It is a novel model integrating critical security technologies and manifesting four necessary features of a secure EHR system. The implementation of the four features is described as follows:

Firstly, the SCBEH model, which optimized a MONA benchmark model and absorbed all its security technologies, has four aspects to be considered: 1) the use of symmetric and asymmetric hybrid encryption technique (KEM-DEM), in which the latest elliptic curve cryptography algorithm (ECC) of asymmetric encryption is used; 2) the applications of group key distribution and group signature technologies are achieved; 3) the revocation and tracking of illegal group members are reimplemented; 4) the computational burden of client is alleviated. Compared with MONA, the proposed model initially achieves the client minimum storage cost reduction of 0 and the client time cost reduction of about 25.9% on generating the 10M file.

Secondly, a two-party session key protocol named password authentication key exchange based on verification elements for lightweight clients (LC-VE-PAKE) is proposed. This protocol enables the client to transfer its computational operations to a specified proxy server securely. Compared with SCBEH without implementing this protocol, the time cost of client users is further reduced on average by 15.8% on generating 10M files, while the time cost of accessing 10M files is significantly reduced by about 10%-79.8%.

Thirdly, an authorization algorithm named federated proxy implements for fine-grained access control based on CP-ABE (FPI-CP-ABE) is proposed. This algorithm verifies the identity and permission of non-group members to meet the strict privacy protection requirements of EHRs data. Compared with the initial SCBEH, the calculation costs of the data owner were all close to 0, while those of the data requester were a little more. Meanwhile, it must be noticed

that the time cost of the data requester on accessing the 10M file is about 0.62s, which is about 13.4% of the proxy server.

Fourthly, an assessment and prediction module named network security situation awareness based on task execution time (TET-NSSA) is proposed to prevent possible security threats timely. The time cost of each component in the security state is extracted as parameters to compute the perceived and predicted values of the security situation of the proposed model. According to the calculated results, the confidence interval of NSSA values on accessing the 10M file is 0.17~0.23. The error between the calculated NSSP values and the measured NSSA values does not exceed 5%.

The results of this study will remarkably facilitate the development of a practical secure cloud-based eHealth system.

Keywords: *E-Health System, Fine-Grained Access Control, Lightweight Clients, Network Security Situation Awareness, Session Key Protocol*

SDG: GOAL 9: Industry, Innovation, and Infrastructure

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KLIEN RINGAN YANG SELAMAT UNTUK MODEL E-KESIHATAN BERASASKAN AWAN

Oleh

ZHANG XIAOWEI

November 2023

Pengerusi : Azizol bin Hj Abdullah, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Keperluan yang tegas untuk keselamatan dan privasi Rekod Kesihatan Elektronik (EHR) adalah isu utama dalam mewujudkan sistem eKesihatan yang selamat. Berdasarkan penyelidikan mod perubatan dan kaji selidik soal selidik ke atas 114 pengamal perubatan dari beberapa hospital tertiari di China, industri perubatan memerlukan sistem EHR berkeselamatan tinggi yang sedemikian, manakala sistem EHR yang digunakan setakat ini tidak dapat memenuhi keperluan tersebut. Penyelesaian kepada kesesakan ini adalah dengan mencadangkan model baharu untuk mewujudkan sistem eKesihatan yang selamat.

Dalam kajian ini, model sistem kesihatan elektronik berasaskan awan selamat (SCBEH) dicadangkan. Ia adalah model baru yang mengintegrasikan teknologi keselamatan kritikal dan menunjukkan empat ciri-ciri penting sistem

EHR yang selamat. Pelaksanaan empat ciri-ciri tersebut diterangkan seperti berikut:

Pertama, model SCBEH, yang mengoptimumkan model penanda aras MONA dan menyerap semua teknologi keselamatannya, mempunyai empat aspek yang perlu dipertimbangkan: 1) penggunaan teknik penyulitan hibrid simetri dan asimetri (KEM-DEM), di mana kriptografi lengkung eliptik terkini algoritma (ECC) penyulitan asimetri digunakan; 2) aplikasi pengedaran kunci kumpulan dan teknologi tandatangan kumpulan dicapai; 3) pembatalan dan pengesanan ahli kumpulan haram dilaksanakan semula; 4) beban pengiraan klien diringankan. Berbanding dengan MONA, model yang dicadangkan pada mulanya mencapai pengurangan kos storan minimum klien sebanyak 0 dan pengurangan kos masa klien sebanyak kira-kira 25.9% apabila menjana fail 10M.

Kedua, pertukaran kunci pengesahan kata laluan protokol kunci sesi dua pihak berdasarkan elemen pengesahan untuk klien ringan (LC-VE-PAKE) dicadangkan. Protokol ini membolehkan klien memindahkan operasi pengiraannya dengan selamat ke pelayan proksi yang ditentukan. Berbanding dengan SCBEH tanpa melaksanakan protokol ini, kos masa pengguna klien dikurangkan lagi secara purata sebanyak 15.8% untuk menjana fail 10M, manakala kos masa untuk mengakses fail 10M dikurangkan dengan ketara sebanyak kira-kira 10%-79.8%.

Ketiga, algoritma kebenaran bersekutu proksi melaksanakan untuk kawalan capaian terperinci berdasarkan CP-ABE (FPI-CP-ABE) dicadangkan.

Algoritma ini mengesahkan identiti dan kebenaran ahli bukan kumpulan untuk memenuhi keperluan perlindungan privasi yang ketat bagi data EHR. Berbanding dengan SCBEH asal, kos pengiraan pemilik data semuanya hampir 0, manakala peminta data adalah lebih sedikit. Sementara itu, perlu diperhatikan bahawa kos masa peminta data untuk mengakses fail 10M adalah kira-kira 0.62s, iaitu kira-kira 13.4% daripada pelayan proksi.

Keempat, modul penilaian dan ramalan yang dinamakan penilaian situasi keselamatan rangkaian berdasarkan masa pelaksanaan tugas digunakan (TET-NSSA) untuk mencegah kemungkinan ancaman keselamatan tepat pada masanya. Kos masa setiap komponen dalam keadaan keselamatan diekstrak sebagai parameter untuk mengira nilai yang dirasakan dan diramalkan bagi situasi keselamatan model yang dicadangkan. Mengikut keputusan yang dikira, selang keyakinan nilai NSSA untuk mengakses fail 10M ialah 0.17~0.23. Ralat antara nilai NSSP yang dikira dan nilai NSSA yang diukur tidak melebihi 5%.

Hasil kajian ini akan memudahkan pembangunan sistem eHealth berasaskan awan selamat yang praktikal.

Kata Kunci: Kawalan Capaian Terperinci, Klien Ringan, Penilaian Keadaan Keselamatan Rangkaian, Protokol Kunci Sesi, Sistem eKesihatan

SDG: *GOAL 9: Industry, Innovation, and Infrastructure*

ACKNOWLEDGEMENTS

First and foremost, I would like to express sincere appreciation to my supervisor, Assoc Prof. Dr. Azizol Abdullah, for his expert guidance, eternal kindness, and steadfast encouragement. I am likewise grateful to my co-supervisors, Assoc Prof. Dr. Mohd Taufik Abdullah and Assoc Prof. Dr. Abdullah Muhammed, for their professional knowledge and valuable assistance. Under their leadership, I have been full of motivation and confident to successfully complete this research.

I thank my dear curriculum teachers and academic lecturers, Prof. Dr.Abdul Azim Abd, Prof. Dr. Rusli Haji Abdullah, Dr. Mohamed Alhadi Mahmoud Alrshah, for their masterly speech, as well as, I also thank my honorific office staffs, Cik Noriah Abdul Malik and Mr. Mohd Haniff Jaffar, for helping me solving academic and laboratory problems.

My sincere appreciation and thanks are also extended to my work unit-Chengde Medical University for the opportunity to further my study as well as the financial supports. In addition, I am most grateful to my colleagues from China and friends in Malaysia. Life abroad is full of joy and enrichment with you accompany.

It is more than a word of thanks that I owe to my mother, my father, and my sister for their continuous support and understanding. Specifically, I am immensely thankful for the everlasting love and respect of my wife Li Lanru, and my son Zhang Manqiu, who spend about five years without my company.

Last but not least, very thanks to Prof. Dr. Zuriati Ahmad Zukarnain, Assoc Prof. Dr. Rohaya Latip, and Prof Dr. Shamala K. Subramaniam for insufficiencies indicated and revision suggested of my thesis. I also particularly thank my colleagues, Li Boning and Wang Danmei, for their explanations on data algorithms and mathematical formulas. All your efforts have been especially helpful to the improvement of my paper.

Thank all of the people who have ever helped me in my life. You are the ones that make my life journey wonderful.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Azizol bin Hj Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Mohd Taufik bin Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Abdullah bin Muhammed, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

_____
ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 18 April 2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABAC	Attribute-based access control model
ABE	Attribute-based encryption
ACP	Access control policy
ACT	Access control tree
AES	Advanced encryption standard
APT	Advanced Persistent Threats
CP-ABE	Ciphertext-policy attribute-based encryption
CSP	Cloud service provider
DAC	Discretionary access control model
DoS	Denial of Service
ECC	Elliptic curve cryptosystem
EHRs	Electronic healthcare records
EMR	Electronic medical record
FPI-CP-ABE	Federated proxy implements for Fine-grained access control based on CP-ABE
HIPAA	The health insurance portability and accountability act
HIS	Hospital information system
HTIM-CN	The healthcare teamwork investigation model in China's tertiary hospitals
IoT	Internet of Things
KEM-DEM	Key encapsulation mechanism - data encapsulation mechanism
KP-ABE	Key-policy attribute-based encryption
LC-VE-PAKE	Password authentication key exchange based on verification element for lightweight clients
MAC	Mandatory access control model

MK	Master key
MONA	Secure multi-owner data sharing for dynamic groups in the cloud
NIST	The national institute of standards and technology, information technology laboratory
NSSA	Network security situation assessment
NSSP	Network security situation prediction
PHRs	Personal healthcare records
PK	Public key
PRE	Proxy re-encryption
RBAC	Role-based access control model
SCBEH	Secure cloud-based electronic health system
SPA	Set pairs analysis
TET-NSSA	Network security situation assessment based on task execution time
UCON	Usage control model
WBDHE	Weak bilinear Diffie-Hellman exponent

CHAPTER 1

INTRODUCTION

1.1 Background

Electronic health records (EHRs) refer to patients' data generated and handled mainly by healthcare professionals, while Personal Health Records (PHRs) refer to measurements such as blood pressure and heart rate, which patients themselves maintain. Both are important and sensitive personal information of relevant patient privacy rights, so the health industry has stringent security regulatory requirements (Pussewalage & Oleshchuk, 2017). The vision of the PHRs system reported by The U.S. Department of Health and Human Services is to "create a PHR that patients, doctors, and other healthcare providers could securely access through the Internet, no matter where a patient is seeking medical care" (Al-Issa, Ottom, & Tamrawi, 2019). The effectiveness of security and privacy control of health information is the most threatening barrier and is still an area of active research within cloud computing (Ali, Shrestha, Soar, & Wamba, 2018). The Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) has been mapped to the Cybersecurity Framework of the National Institute of Standards and Technology (NIST, 2017), which can be used to help organizations to assess the completeness of their cybersecurity programs (CMU/SEI-2018-TN-001).

Teamwork in healthcare settings is widely recognized as essential in the medical industry (Valentine, Nembhard, & Edmondson, 2014). Nurse-

physician collaboration is mainly embodied in sharing patient information. In contrast, collaboration failures, such as the doctor ignoring the nurse's response to checking drugs, would result in clinical errors (Y. Wang et al., 2018, Fang, Feng, & Xu, 2018). The medical laboratory's diagnoses are also critical (Tam, Chi-shing Cho, & Bun Ng, 2018). Understanding a natural medical environment with EHRs is the premise of this research, for which a questionnaire including questions such as team size, EHRs access frequency, and EHRs survival time was conducted in several China tertiary hospitals involving 114 medical practitioners. The questionnaire is arranged in Appendix A, and the analysis of collected data is arranged in Appendix B.

Because cloud computing architecture consists of different types of distributed systems, service security, rational computing overhead and access control management are three necessary mechanisms (Indu, Anand, & Bhaskar, 2018). In terms of security, encryption on highly private data, which enables secure accessing and sharing over the network, is critical to eHealth's success (Edemacu, Park, Jang, & Kim, 2019), while an online/offline encryption scheme was proposed, which was equipped with the Attribute-Based Encryption (ABE) technique for realizing fine-grained data sharing and security protection (Jin Li, Zhang, Chen, & Xiang, 2018). In terms of computing overhead, an access control EHR model was proposed, in which complex computation of senders and receivers was outsourced to public cloud servers, suiting inexpensive mobile phones with constrained resources (Ma et al., 2020). Similarly, a model used two servers for proxy re-encryption and receiver verification, respectively, to reduce the computational burden on the user side

(Zhan et al., 2020). In terms of access control, an attribute-based authorization mechanism was used to authorize users who access EHR resources (Pussewalage & Oleshchuk, 2017). As an extension of cloud computing, ciphertext operations were carried out by fog computing for achieving thin clients so that more resource-constrained devices could join the cloud computing platform (P. Zhang, Chen, Liu, Liang, & Liu, 2018). Furthermore, A solution for security monitoring and analysis functions was implemented by highlighting the outliers created by rejecting certain legitimate activities (Cogranne, Doyen, Ghadban, & Hammi, 2018).

Thin-client realization is to reduce its computing burden under the premise with an excellent security scheme, and an attribute-based authorization mechanism can be used to authorize users who access EHR resources while utilizing a proxy re-encryption scheme to facilitate users' decryption operation (Pussewalage & Oleshchuk, 2017). The security of this mechanism was proven able to resist collusive attacks. A scheme was proposed leaving only one modular exponentiation to the client for realizing security (R. Zhang, Ma, & Lu, 2017). A scheme was proposed to revoke and update user credentials by Cloud Service Providers (CSPs) to deal with the secure access of dynamic user groups (Xu, Yang, Mu, & Deng, 2018). Besides, in a biometric identification outsourcing scheme, users' biometric data are encrypted by data owners and then submitted to the cloud, which can resist collusive attacks of illegal users and CSP (Zhu, Zhang, Xu, Liu, & Huang, 2018). An asymmetric three-party-based authentication scheme was proposed utilizing the visual out-of-band (OOB) channel, two-dimensional codes (QR codes), and the secure

device pairing method (S. Liu, Hu, Weng, Zhu, & Chen, 2016). Furthermore, a mutual authentication scheme was proposed to establish secret session keys for secure communication between users and wearable sensor nodes (Jangirala, Das, Kumar, & Rodrigues, 2020). A publication-subscription lightweight protocol was proposed between Fog and IoT nodes (Diro, Chilamkurti, & Kumar, 2017).

A secure scheme developed by IRCCS "Bonino Pulejo" clinical and research center (Italy) was discussed, in which clinical data can be authorized to clinical operators who match the settled access policy (Galletta et al., 2017). Dynamic user management was realized by allowing a data owner to re-encrypt his data using his private attribute key, tantamount to changing the authorization object (H. Cui, Deng, & Li, 2018). A black-box accountable CP-ABE scheme was proposed for malicious users, which can trace malicious users through an embedded secret value in a key generated for an auditing ciphertext (Z. Liu, Ding, Yuan, & Wang, 2023). Accumulator-based encryption integrating with CP-ABE was introduced to achieve an additional black box traceability feature by just adding the O(1) element to the ciphertext and the public key (Song, Wu, & Huang, 2010). A particular attribute "id" provided and saved by a specified component "manager" was employed for tracing and revoking malicious users (Premkamal, Pasupuleti, & Alphonse, 2021). Regarding relevant algorithms, the Merkle hash tree was used to achieve fine-grained access control (Xue et al., 2019). A scheme was proposed for multi-authority models to dynamically remove any user from its authorized access domain (Wei, Liu, & Hu, 2018). An Elliptic Curve Cryptography-based CP-ABE scheme was adopted for IoT-

enabled healthcare systems, using multiple attribute authorities responsible for user certificates to perform authentication tasks (Das & Namasudra, 2023).

Network Security Situation Awareness (NSSA) is an integral part of cybersecurity defense and is essential for managers to respond to increasingly sophisticated cyber threats (J. Zhang, Feng, Liu, & Zhao, 2023). A method was proposed to classify security factors as awareness indexes and further process them hierarchically for predicting security situations on a grey neural network (Shen & Wen, 2019). A method based on the Bayesian game model was proposed for identifying fake feedback values (Siadat, Rahmani, & Navid, 2017), while a general model was presented to explain how disinformation can be used to monitor and resist Advanced Persistent Threats (APTs) (Ahmad, Webb, Desouza, & Boorman, 2019). NSSA technologies are versatile, and a method used in distribution networks was proposed, in which weight values of situation indexes were calculated based on a data mining technology named the convolution-gating cyclic network (N. Wang, Han, & Wang, 2023). An awareness model was designed for a multi-element integrated power grid based on the fusion processing of massive heterogeneous measurement data (Qian & Xu, 2023). It was highlighted that the focus of NSSA research would move from fundamental principles to applied research and experimental development (Husák, Jirsík, & Yang, 2020). A laboratory insider detection system was proposed for monitoring IP and physical addresses accessing irrelevant websites illegally (Yamin, Katt, Sattar, & Ahmad, 2020), and a detection strategy on sensor networks was proposed to defeat Hello flooding

attacks by making a statistic analysis of the amount of packet loss (Gill & Sachdeva, 2018).

1.2 Problem statement

Based on the questionnaire survey, relevant regulations, and related research on the usage of EHR, the requirements of a secure eHealth model development are learned, such as the working methods of medical team collaboration and information sharing (Y. Wang et al., 2018), the mapping standard of medical information usage security rules (HIPAA) to network security frameworks (NIST, 2017), the importance of EHR encryption (Edemacu et al., 2019), the widespread use of resource-constrained devices by the EHRs model terminals (Ma et al., 2020), the inevitability of shifting the computational burden on clients (Pussewalage & Oleshchuk, 2017), and the necessity of user authentication for accessing EHR (Das & Namasudra, 2023). The benchmark model MONA was chosen because it is configured with basic security mechanisms and implements some of the above functions. Specifically, MONA's security mechanism adopts the latest symmetric encryption algorithm AES and asymmetric encryption algorithm ECC and their hybrid use, group key distribution and group member sharing of encrypted files, group file signature and verification, and user verification; The seven essential functions implemented by MONA include security system initialization, user registration, member revocation, file ciphertext generation, file deletion, file access control, and illegal user tracking. However, for an eHealth system with strict security requirements, the MONA model could be better in four aspects:

model component composition, thin client, secure communication, and self-security monitoring, which are needed to be optimized and improved. Below, we will elaborate on these four aspects separately.

An eHealth system faces challenges such as data security protection, flexible data sharing, efficient authority delegation, computation efficiency optimization, Etc. (Ma et al., 2020). A model's primary work is to design components' functions as well as solutions for security and privacy protection (Tabrizchi & Kuchaki Rafsanjani, 2020). Cryptographic mechanisms apply security measures directly to the data, and better functions can be achieved through appropriate cryptographic suites (Indu et al., 2018). Attribute-Based Encryption (ABE) is a necessary ingredient and the most suitable candidate for the eHealth system (Edemacu et al., 2019). Outsourced ABE can vastly reduce the computation cost for users (Jiguo Li, Lin, Zhang, & Han, 2017), while the proxy re-encryption scheme and support verification can reduce users' computational burden (Zhan et al., 2020). In brief, a secure model with a thin client is crucial in implementing an excellent cloud-based eHealth system. However, the component structure setting of the benchmark model MONA needs to be revised, resulting in unnecessary storage and a heavy computational burden on the client. Therefore, the MONA model is to be optimized as a thin-client model with a proxy server, which can transfer the client's storage cost and computing burden. This is the key to achieving an excellent cloud-based eHealth system.

Measures supporting secret transfer of information is very necessary (Venkatesan, 2023). Password authenticated Key exchange which allows two parties with a shared password to establish a session key is considered one of the most secure transmission methods (Lian, Yang, & Zhao, 2022). An enhanced key generation technique was implemented with the use of string comparison based on Diffie-Hellman key exchange algorithm (Prabahar, Sukumar, & SureshBabu, 2022). A protocol was presented through employing biometric resilient authenticated key exchange (Silde et al., 2022). A zero-knowledge proofs-based authenticated key agreement protocol was proposed for the Internet of healthcare applications (Gaba et al., 2022), while a lightweight and secure key exchange scheme was presented based on ECC for fog federation environments (Salami & Khajehvand, 2021). In summary, it is necessary to design a password authenticated key exchange protocol for communication between thin-clients and other components. Given the important role of authentication protocols, it is necessary to develop a session key between the proxy server and the client to ensure secure communication security between them, thereby further transferring operations except file symmetric encryption and decryption to the proxy server for execution as much as possible.

Ciphertext-policy attribute-based encryption for the eHealth system can effectively serve medical professionals to achieve fine-grained sharing of EHRs (Z. Liu et al., 2023). A Merkle tree-based access structure was proposed to allow a data requester to obtain access permission after providing only the correct attributes being verified by hashed values of tree nodes (Reddy &

Adilakshmi, 2023). An access tree-based mechanism combining ECC was adopted to achieve higher efficiency (Sammy & Vigila, 2022). A multi-authority CP-ABE access scheme was proposed to re-encrypt the data involving access attribute revocation to revoke some users' access permissions (Das & Namasudra, 2022). However, this model was computationally heavy. A multi-authority traceable and revocable ABE system was proposed (Sethi, Pradhan, & Bera, 2021). However, some components can be removed without compromising security, and its computational burden was very high. To solve the problems mentioned above, a flexible, scalable, and efficient fine-grained access control scheme is desired in this study. Due to the inability of the MONA model to use the group key distribution scheme to authorize non-group members to access group-shared files, it is necessary to design a fine-grained access control scheme based on CP-ABE in our proposed model to meet the flexible authorization of file owners for non-group members to access group sharing files.

The critical research on NSSA, which reflects the security status of the entire network, depends on the relevance of the extracted situation values of the main elements (Manickam & Chong, 2015). Network Security Situation Prediction (NSSP) is the next stage of NSSA and can predict the following few situations change (Xi, Jin, Yun, & Zhang, 2011). A risk index system including 240 secondary indicators of situational awareness was constructed to assess the whole-link network status using the logistic regression model (Sun, Deng, & Du, 2022). A zero-trust architecture was proposed to extract indexes from four dimensions, subject, object, behavior, and environment, to achieve the

real-time NSSA and NSSP system of the 5G smart healthcare platform (B. Chen et al., 2021). In terms of the algorithms used, an approach was proposed based on both entropy and packet number time series for testing distributed Denial-of-Service in an academic network (Bojović, Bašičević, Ocovaj, & Popović, 2019). A prediction approach was proposed via data set handling of tracking time series from elements (Nguyen, Lee, Nguyen-Xuan, & Lee, 2019). However, its efficiency was achieved at the expense of tracking time. Therefore, our proposed model's reliable awareness and prediction module is essential. Summing up the above, designing a reliable perception and prediction module for our proposed model is necessary, while MONA lacks this security mechanism.

1.3 Research objectives

According to the problems stated above, the research objectives of this study are as follows:

- To propose a cloud-based eHealth model with reasonable components and comprehensive security measures to reduce time and storage costs on the client side.
- To propose a password authentication key exchange protocol for securing communication by reducing time and storage costs between thin client and proxy server.

- To propose a fine-grained access control scheme that can perform flexible authorization of potential data requesters.

- To propose a network security situation awareness and prediction module that can enhance the proposed model security.

1.4 Research significance

The main significance of this study is firstly to propose a novel model suitable for cloud-based eHealth systems on the premise of completely understanding the requirements of the medical environment by organizing a detailed questionnaire on medical practitioners. Furthermore, we targeted our research in three aspects: realizing a lightweight thin-client protocol, designing a fine-grained access control scheme, and proposing an awareness and prediction module. The results of this research will remarkably facilitate the implementation of the practical eHealth system.

1.5 Thesis contribution

Our contributions to this thesis are based on four aspects. Firstly, we propose a novel secure eHealth model of implementing basic, excellent security measures such as dynamic broadcast group application, reasonable usage of asymmetric and symmetric encryption algorithms, necessary security verification, and so forth. Secondly, with a full understanding of the widespread application of resource-restricted portable devices in medical environments, this proposed model further focuses on the thin-client design with a specific

protocol that matches the above-mentioned security measures to ensure communication security. Thirdly, we design a fine-grained access control scheme with patients as the center to authorize uncertain dynamic users who have requirements for access to EHRs, and with the quality of being compatible with the above-stated security measures. Fourthly, we have designed a network security situation awareness and prediction module that can ensure the integral security of this proposed model.

In summary, the main contributions of this study can be summarized as follows:

- Development of a novel security cloud-based eHealth model, SCBEH, which is used for reducing storage and time costs for the client;
- Development of an authentication and key exchange protocol, LC-VE-PAKE, which is used for secure communication between client and proxy server;
- Development of a scheme, FPI-CP-ABE, which is used for implementing fine-grained access control authorization over non-group members;
- Development of a module, TET-NSSA, which is used for realizing security situation awareness and prediction on this proposed model.

1.6 Thesis organization

This thesis comprises five chapters, the remaining ones are listed as follows:

Chapter 2 is about a literature review. The methodologies for the proposed SCBEH model and the results of re-implementing the benchmark model MONA are demonstrated in Chapter 3. Then, the detailed description, implementations, and results of the four proposals, which are the preliminary optimization of MONA model, the LC-VE-PAKE protocol, the FPI-CP-ABE scheme, and the TET-NSSA module, are demonstrated and discussed in Chapter 4, Chapter 5, Chapter 6, and Chapter 7, respectively. Finally, the conclusion and future work are stated in Chapter 8. It must be supplemented that a questionnaire is arranged in Appendix A, and the collected data with analyses are arranged in Appendix B.

REFERENCES

Adrián Sánchez-Carmona, Robles, S., & Borrego, C. (2016). Identity-based access control for pro-active message's DTN. *Security And Communication Networks*, *9*, 2323–2337.

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers and Security*, *86*, 402–418.

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: A survey. *Journal of Healthcare Engineering*, *2019*.

Alam, Q., Tabbasum, S., Malik, S. U. R., Alam, M., Ali, T., Akhunzada, A., Buyya, R. (2016). Formal verification of the xDAuth protocol. *IEEE Transactions on Information Forensics and Security*, *11*(9), 1956–1969.

Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: Issues and current solutions. *International Journal of Advanced Computer Science and Applications*, *7*(4), 485–498.

Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, *43*(July), 146–158.

Alsayegh, M., Moulahi, T., Alabdulatif, A., & Lorenz, P. (2022). Towards secure searchable electronic health records using consortium blockchain. *Network*, *2*(2), 239–256.

Arnaut, U., Tair, M., & Veinović, M. (2021). Comparison of the efficiency of aes implementations on major web platforms. *In Sinteza 2021-International Scientific Conference on Information Technology and Data Related Research* (pp. 153-157). Singidunum University.

Au, M. H., Liang, K., Liu, J. K., Lu, R., & Ning, J. (2018). Privacy-preserving personal data operation on mobile cloud—Chances and challenges over advanced persistent threat. *Future Generation Computer Systems*, *79*, 337–349.

Bahar, A. Y., Shorman, S. M., Khder, M. A., Quadir, A. M., & Almosawi, S. A. (2022). Survey on features and comparisons of programming languages (PYTHON, JAVA, AND C#). *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2022*, 154–163.

Baig, M. M., GholamHosseini, H., & Connolly, M. J. (2015). Mobile healthcare applications: system design review, critical issues and challenges.

Australasian Physical and Engineering Sciences in Medicine, *38*(1), 23–38.

Ben, L., Dan, B., & Hanav, S. (2004). Short signature from the weil pairing. *J. Cryptology*, *Vol.17,No.*, 1–24.

Bethencourt, J., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. *IEEE Symposium on Security and Privacy(SP07)*.

Bhaskaran, S. M., & Sridhar, R. (2017). Hybrid solution for privacy-preserving access control for healthcare data. *Advances in Electrical and Computer Engineering*, *17*(2), 31–38.

Bojović, P. D., Bašičević, I., Ocovaj, S., & Popović, M. (2019). A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. *Computers and Electrical Engineering*, *73*, 84–96.

Boneh, D., Boyen, X., & Goh, E. J. (2005, May). Hierarchical identity based encryption with constant size ciphertext. *In Annual international conference on the theory and applications of cryptographic techniques* (pp. 440-456).

Boneh, D., & Franklin, M. (2003). Identity-Based Encryption from the Weil Pairing. *SIAM Journal on Computing*, *32*(3), 586–615.

Carayon, P., Schoofs Hundt, A., Karsh, B. T., Gurses, A. P., Alvarado, C. J., Smith, M., & Brennan, P. F. (2006). Work system design for patient safety: The SEIPS model. *Quality and Safety in Health Care*, *15*(SUPPL. 1), 50–58.

Carayon, Pascale, Wetterneck, T. B., Rivera-Rodriguez, A. J., Hundt, A. S., Hoonakker, P., Holden, R., & Gurses, A. P. (2014). Human factors systems approach to healthcare quality and patient safety. *Applied Ergonomics*, *45*(1), 14–25.

Carniani, E., D'Arenzo, D., Lazouski, A., Martinelli, F., & Mori, P. (2016). Usage control on cloud systems. *Future Generation Computer Systems*, *63*, 37–55.

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., … Zhai, Y. (2021). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), 10248–10263.

Chen, Y., Yao, T., Ren, H., & Gan, Z. (2022). Unidirectional identity-based proxy re-signature with key insulation in EHR sharing system. *CMES - Computer Modeling in Engineering and Sciences*, *131*(2).

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-Health solutions in cloud computing. *IEEE Access*, *7*, 74361–74382.

Chowdhury, Z. J., Pishva, D., & Nishantha, G. G. D. (2010). AES and confidentiality from the inside out. *Advanced Communication Technology (ICACT), 2010 The 12th International Conference On*, *2*, 1587–1591.

Cogranne, R., Doyen, G., Ghadban, N., & Hammi, B. (2018). Detecting botclouds at large scale: A decentralized and robust detection method for multi-tenant virtualized environments. *IEEE Transactions on Network and Service Management*, *15*(1), 68–82.

Cui, H., Deng, R. H., & Li, Y. (2018). Attribute-based cloud storage with secure provenance over encrypted data. *Future Generation Computer Systems*, *79*, 461–472.

Cui, J., Li, B., Zhong, H., Xu, Y., & Liu, L. (2022). Achieving revocable attribute group-based encryption for mobile cloud data: A multi-proxy assisted approach. *IEEE Transactions on Dependable and Secure Computing*, *PP*, 1–14.

Cuppens-Boulahia, N., Cuppens, F., Tawbi, N., & Wang, L. (2017). Preface. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10128 LNCS*, VI.

Das, S., & Namasudra, S. (2022). MACPABE: Multi-authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure. *International Journal of Network Management*, (November 2021), 1–20.

Das, S., & Namasudra, S. (2023). Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure. *IEEE Transactions on Industrial Informatics*, *19*(1), 821–829.

Delerabl´, C., Paillier, P., & Pointcheval, D. (2007). Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. *In International Conference on Pairing-Based Cryptography*, *Springer,*(july), 39–59.

Diro, A. A., Chilamkurti, N., & Kumar, N. (2017). Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing. *Mobile Networks and Applications*, *22*(5), 848–858.

Doukas, C., Pliakas, T., & Maglogiannis, I. (2010). Mobile healthcare information management utilizing cloud computing and android OS. In Engineering in Medicine and Biology Society (EMBC). *2010 Annual International Conference of the IEEE*, 1037–1040.

Duela, J. S., Suresh, A. B., & Umamaheswari, P. (2015). Asymmetric encryption to secure multi-proprietor data sharing for activemembers in cloud. *2014 International Conference on Information Communication and Embedded Systems, ICICES 2014*, (978), 1–5.

Edemacu, K., Park, H. K., Jang, B., & Kim, J. W. (2019). Privacy provision in collaborative eHealth with attribute-based encryption: Survey, challenges and future directions. *IEEE Access*, *7*, 89614–89636.

Elmisery, A. M., Rho, S., & Aborizka, M. (2019). A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. *Cluster Computing*, *22*, 1611–1638.

Fugkeaw, S. (2023). Secure data sharing with efficient key update for industrial cloud-based access control. *IEEE Transactions on Services Computing*, *16*(1), 575–587.

Fugkeaw, S., & Sato, H. (2017). Improved lightweight proxy re-encryption for flexible and scalable mobile revocation management in cloud computing. *IEEE International Conference on Cloud Computing, CLOUD*, 894–899.

Gaba, G. S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M., & Alazab, M. (2022). Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. *Sustainable Cities and Society*, *80*(February), 103766.

Galletta, A., Bonanno, L., Celesti, A., Marino, S., Bramanti, P., & Villari, M. (2017). An approach to share MRI data over the cloud preserving patients' privacy. *Proceedings - IEEE Symposium on Computers and Communications*, (Iscc), 94–99.

Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, *36*(6), 1161–1173.

Gill, R. K., & Sachdeva, M. (2018). Detection of hello flood attack on LEACH in wireless sensor networks. *Advances in Intelligent Systems and Computing*, *638*, 377–387.

Gjerdrum, A. T., Johansen, H. D., & Johansen, D. (2016). Implementing informed consent as information-flow policies for secure analytics on eHealth data: Principles and practices. *Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016*, 107–112.

He, H., Zhang, W., Liu, C., & Sun, H. (2020). Trustworthy enhancement for cloud proxy based on autonomic computing. *IEEE Transactions on Cloud Computing*, *8*(4), 1108–1121.

Hu, G., & Qiao, P. (2016). Cloud belief rule base model for network security situation prediction. *IEEE Communications Letters*, *20*(5), 914–917.

Hu, G., Zhou, Z., Zhang, B., Yin, X., & Gao, Z. (2016). A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm. *Applied Soft Computing Journal*, *48*, 404–418.

Husák, M., Jirsík, T., & Yang, S. J. (2020). SoK: Contemporary issues and challenges to enable cyber situational awareness for network security. *ACM International Conference Proceeding Series*.

Ibrahim, A., Mahmood, B., & Singhal, M. (2016). A secure framework for sharing electronic health records over clouds. *2016 IEEE International Conference on Serious Games and Applications for Health, SeGAH 2016*, 1–8.

Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, *21*(4), 574–588.

Jangirala, S., Das, A. K., Kumar, N., & Rodrigues, J. J. P. C. (2020). Cloud centric authentication for wearable healthcare monitoring system. *IEEE Transactions on Dependable and Secure Computing*, *17*(5), 942–956.

Jiang, S., Zhu, X., & Wang, L. (2015). EPPS: Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks. *Sensors (Switzerland)*, *15*(9), 22419–22438.

Jiang, Y., Xu, X., & Xiao, F. (2022). Attribute-based encryption with blockchain protection scheme for electronic health records. *IEEE Transactions on Network and Service Management*, *19*(4), 3884–3895.

Kaffel-Ben Ayed, H., & Zaghdoudi, B. (2016). A generic Kerberos-based access control system for the cloud. *Annales Des Telecommunications/Annals of Telecommunications*, *71*(9–10), 555–567.

Kaur, J., Rani, R., & Kalra, N. (2022). A blockchain-based framework for privacy preservation of electronic health records (EHRs). *Transactions on Emerging Telecommunications Technologies*, *33*(9), 1–18.

Kim, S. H., & Lee, I. Y. (2018). IoT device security based on proxy re-encryption. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 1267–1273.

Li, Jiguo, Lin, X., Zhang, Y., & Han, J. (2017). KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage. *IEEE Transactions on Services Computing*, *10*(5), 715–725.

Li, Jin, Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers and Security*, *72*, 1–12.

Li, R., Shen, C., He, H., & Gu, X. (2018). A lightweight secure data sharing scheme for mobile cloud computing. *IEEE Transactions on Cloud Computing*, *6*(2), 344–357.

Li, W., Liu, K., Yang, H., & Yu, C. (2014). Integrated clinical pathway management for medical quality improvement - based on a semiotically inspired systems architecture. *European Journal of Information Systems*, *23*(4), 400–417.

Lian, H., Yang, Y., & Zhao, Y. (2022). Efficient and strong symmetric password authenticated key exchange with identity privacy for IoT. *IEEE Internet of Things Journal*, *10*(6), 4725–4734.

Lin, H.-Y. (2018). Traceable anonymous authentication and key exchange protocol for privacy-aware cloud environments. *IEEE Systems Journal*, *PP*, 1–10.

Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L., & Chen, J. (2015). MuR-DPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud. *IEEE Transactions on Computers*, *64*(9), 2609–2622.

Liu, S., Hu, S., Weng, J., Zhu, S., & Chen, Z. (2016). A novel asymmetric three-party based authentication scheme in wearable devices environment. *Journal of Network and Computer Applications*, *60*, 144–154.

Liu, Z., Ding, Y., Yuan, M., & Wang, B. (2023). Black-box accountable authority CP-ABE scheme for cloud-assisted eHealth system. *IEEE Systems Journal*, *17*(1), 756–767.

Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2016). Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Future Generation Computer Systems*, *55*, 266–277.

Ma, H., Zhang, R., Yang, G., Song, Z., He, K., & Xiao, Y. (2020). Efficient fine-grained data sharing mechanism for electronic medical record systems with mobile devices. *IEEE Transactions on Dependable and Secure Computing*, *17*(5), 1026–1038.

Manickam, Y. L. S., & Chong, Y. (2015). Network security situation assessment : *Information Science and Applications*, *Lecture Notes in Electrical Engineering 339*, 407–414.

Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2016). Security challenges in healthcare cloud computing: A systematic review. *Global Journal of Health Science*, *9*(3), 157.

Nguyen, T. N., Lee, S., Nguyen-Xuan, H., & Lee, J. (2019). A novel analysis-prediction approach for geometrically nonlinear problems using group method of data handling. *Computer Methods in Applied Mechanics and Engineering*, *354*, 506–526.

Ogala, J., & State, D. (2022). Comparative analysis of c , c ++ , c # and java programming gsj : Volume 8 , Issue 5 , May 2020 , Online : ISSN 2320-9186, (February).

Pardeshi, M. S., Sheu, R. K., & Yuan, S. M. (2022). Hash-chain fog/edge: A mode-based hash-chain for secured mutual authentication protocol using zero-knowledge proofs in fog/edge. *Sensors*, *22*(2).

Prabahar, L., Sukumar, R., & SureshBabu, R. (2022). CCSC—DHKEP: Data confidentiality using improved security approaches in cloud environment. *Wireless Personal Communications*, *122*(4), 3633–3647.

Premkamal, P. K., Pasupuleti, S. K., & Alphonse, P. J. A. (2021). Dynamic traceable CP-ABE with revocation for outsourced big data in cloud storage. *International Journal of Communication Systems*, *34*(2), 1–21.

Pussewalage, H. S. G., & Oleshchuk, V. A. (2017). A patient-centric attribute based access control scheme for secure sharing of personal health records using cloud computing. *Proceedings - 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, IEEE CIC 2016*, 46–53.

Qian, J., & Xu, H. (2022). Research on network security situational awareness technology for building multi-element, integrated and highly elastic power grid, 424–428.

Rachmat, N., & Samsuryadi. (2019). Performance analysis of 256-bit aes encryption algorithm on android smartphone. *Journal of Physics: Conference Series*, *1196*(1).

Reddy, B. R., & Adilakshmi, T. (2023). Proof-of-work for merkle based access tree in patient centric data. *International Journal of Advanced Computer Science and Applications*, *14*(1), 533–539.

Roy, R., & P., P. (2017). Proxy re-encryption schemes for secure cloud data and applications: A survey. *International Journal of Computer Applications*, *164*(5), 1–6.

Salami, Y., & Khajehvand, V. (2021). LSKE: Lightweight secure key exchange scheme in fog federation. *Complexity*, *2021*(i).

Salnikova, N. A., Lempert, B. A., & Lempert, M. B. (2015). Integration of methods to quantify the quality of medical care in the automated processing systems of medical and economic information natalia. *Communications in Computer and Information Science*, *535*, 307–319.

Sammy, F., & Vigila, S. M. C. (2022). An efficient blockchain based data access with modified hierarchical attribute access structure with CP-ABE using ECC scheme for patient health record. *Security and Communication Networks*, *2022*.

Santana, M., & Guan, L. (2016). Infrastructure as a service: exploring network access control challenges. *SAI Computing Conference*, 37–46.

Sethi, K., Pradhan, A., & Bera, P. (2021). PMTER-ABE: a practical multi-authority CP-ABE with traceability, revocation and outsourcing decryption for secure access control in cloud systems. *Cluster Computing*, *24*(2), 1525–1550.

Shamsolmoali, P., & Alam, M. A. (2015). Ensuring data security and performance evaluation in cloud computing. *Intelligent Computing, Communication and Devices*, *308 AISC*(VOLUME 1), 415–423.

Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. *IEEE Communications Magazine*, *55*(9), 78–85.

Shen, L., & Wen, Z. (2019). Network security situation prediction in the cloud environment based on grey neural network. *Journal of Computational Methods in Sciences and Engineering*, *19*(1), 153–167.

Shynu, P. G., & John Singh, K. (2016). A comprehensive survey and analysis on access control schemes in cloud environment. *Cybernetics and Information Technologies*, *16*(1), 19–38.

Siadat, S., Rahmani, A. M., & Navid, H. (2017). Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model. *Journal of Supercomputing*, *73*(6), 2682–2704.

Silde, T., Poljuha, M., Tullot, A., Costache, A., Rathgeb, C., ... & Busch, C. (2022). BRAKE: Biometric resilient authenticated key exchange. *Cryptology ePrint Archive*

Singh, M. G., Singla, M. A., & Sandha, M. K. (2011). Cryptography algorithm comparison for security enhancement in wireless intrusion detection system. *International Journal of Multidisciplinary Research, 1(4),* 143-151.

Singh, Gurpreet, & Supriya, S. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, *67*(19), 33–38.

Song, P., Wu, Q., & Huang, Y. (2010). Multidisciplinary team and team oncology medicine research and development in China. *BioScience Trends.*, *4*(4), 151–160.

Sun, J., Deng, F., & Du, B. (2022). Research on whole-link risk situational awareness index system and dynamic risk pool supervision. *ACM International Conference Proceeding Series*, 190–197.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *Journal of Supercomputing* (Vol. 76). Springer US.

Tam, C., Chi-shing Cho, W., & Bun Ng, T. (2018). Elements of effective practice in patient-centred laboratory medicine. *Preventive Medicine and Community Health*, *1*(1), 1–6.

Tang, Y., & Elhoseny, M. (2019). Computer network security evaluation simulation model based on neural network. *Journal of Intelligent and Fuzzy Systems*, *37*(3), 3197–3204.

Tseng, Y.-M., Chen, J.-L., & Huang, S.-S. (2021). A lightweight leakage-resilient identity-based mutual authentication and key exchange protocol for resource-limited devices. *Computer Networks*, *196*(June 2020), 108246.

Vaidya, A. S., Srinivas, M. B., Himabindu, P., & Jumaxanova, D. (2013). A smart phone/tablet based mobile health care system for developing countries. *Conference Proceedings : Annual International Conference of the IEEE Engineering in Medicine and Biology Society. 2013*, 4642–4645.

Valentine, M. a, Nembhard, I. M., & Edmondson, A. C. (2014). Measuring teamwork in health care settings: A review of survey instruments. *Medical Care*, *00*(00), 1–15.

Venkatesan, S. (2023). Identification protocol heterogeneous systems in cloud computing. *Mathematical Statistician and Engineering Applications*, 72(1), 615-621.

Vidhya, S., & Kalaivani, V. (2023). A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. *Peer-to-Peer Networking and Applications*, 900–913.

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*(xxxx), 2172–2175.

Wady, S. H., & Yousif, R. Z. (2022). A secure medical image transmission system based on 2D logistic map and Diffie-Hellman key exchange mechanisms. *UHD Journal of Science and Technology*, *6*(2), 94–104.

Wang, N., Han, H., & Wang, X. (2023). Situation awareness method of distribution network operation based on data mining technology. *2022 4th*

International Academic Exchange Conference on Science and Technology Innovation (IAECST), 923–927.

Wang, Y., Wan, Q., Guo, J., Jin, X., Zhou, W., Feng, X., & Shang, S. (2018). The influence of effective communication, perceived respect and willingness to collaborate on nurses' perceptions of nurse–physician collaboration in China. *Applied Nursing Research*, *41*, 73–79.

Wei, J., Liu, W., & Hu, X. (2018). Secure and efficient attribute-based access control for multiauthority cloud storage. *IEEE Systems Journal*, *12*(2), 1731–1742.

West, M. A., & Lyubovnikova, J. (2013). Illusions of team working in health care. *Journal of Health Organization and Management*, *27*(1), 134–142.

Wu, R., Ahn, G.-J., & Hu, H. (2012). Secure sharing of electronic health records in clouds. *Proceedings of the 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 711–718.

Xi, R., Jin, S., Yun, X., & Zhang, Y. (2011). CNSSA : A comprehensive network security situation awareness system. *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, 482–487.

Xu, S., Yang, G., Mu, Y., & Deng, R. H. (2018). Secure fine-grained access control and data sharing for dynamic groups in the cloud. *IEEE Transactions on Information Forensics and Security*, *13*(8), 2101–2113.

Xue, L., Yu, Y., Li, Y., Au, M. H., Du, X., & Yang, B. (2019). Efficient attribute-based encryption with attribute revocation for assured data deletion. *Information Sciences*, *479*, 640–650.

Yamin, M. M., Katt, B., Sattar, K., & Ahmad, M. Bin. (2020). Implementation of insider threat detection system using honeypot based sensors and threat analytics. *Lecture Notes in Networks and Systems* (Vol. 70). Springer International Publishing.

Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health internet of things. *Journal of Network and Computer Applications*, *89*(November 2016), 26–37.

Yuan, X., Wang, X., Wang, J., Chu, Y., Wang, C., Wang, J., … Liu, S. (2016). Enabling secure and efficient video delivery through encrypted in-network caching. *IEEE Journal on Selected Areas in Communications*, *34*(8), 2077–2090.

Yuen, T. H., Liu, J. K., Au, M. H., Huang, X., Susilo, W., & Zhou, J. (2014). $ K $-times attribute-based anonymous access control for cloud computing. *IEEE Transactions on Computers*, *64(9),* 2595-2608

Zeng, W., Yang, Y., & Luo, B. (2015). Content-based access control: Use data content to assist access control for large-scale content-centric databases. *Proceedings - 2014 IEEE International Conference on Big Data, IEEE Big Data 2014*, 701–710.

Zhan, Y., Wang, B., Wang, Z., Pei, T., Chen, Y., Qu, Q., & Zhang, Z. (2020). Improved proxy re-encryption with delegatable verifiability. *IEEE Systems Journal*, *14*(1), 592–602.

Zhang, J., Feng, H., Liu, B., & Zhao, D. (2023). Survey of technology in network security situation awareness. *Sensors*, *23*(5), 1–25.

Zhang, P., Chen, Z., Liu, J. K., Liang, K., & Liu, H. (2018). An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Future Generation Computer Systems*, *78*, 753–762.

Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. *Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*, 268–275.

Zhang, R., Ma, H., & Lu, Y. (2017). Fine-grained access control system based on fully outsourced attribute-based encryption. *Journal of Systems and Software*, *125*, 344–353.

Zhang, Y., Wang, B., & Yan, J. (2013). Mona : Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud. *IEEE Transactions on Parallel and Distributed Systems*, *24*(6), 1182–1191.

Zhao, Chuan, Zhao, S., Zhang, B., Jing, S., Chen, Z., & Zhao, M. (2019). Towards secure computation of similar patient query on genomic data under multiple keys. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 11983 LNCS). Springer International Publishing.

Zhao, Chun, Wang, L., & Zhang, X. (2020). Service agent networks in cloud manufacturing: Modeling and evaluation based on set-pair analysis. *Robotics and Computer-Integrated Manufacturing*, *65*(March), 101970.

Zhou, S., Chen, G., Huang, G., Shi, J., & Kong, T. (2020). Research on multi-authority CP-ABE access control model in multicloud. *China Communications*, *17*(8), 220–233.

Zhou, Z., & Huang, D. (2012). Efficient and Secure Data Storage Operations for Mobile Cloud Computing. *2012 8th International Conference on Network and Service Management (Cnsm) and 2012 Workshop on Systems Virtualiztion Management (Svm)*, 37–45.

Zhu, L., Zhang, C., Xu, C., Liu, X., & Huang, C. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. *IEEE Access*, *6*, 19025–19033.