TOWARD EFFICIENT ATTRIBUTE-BASED SEARCHABLE ENCRYPTION FOR ACCESS CONTROL OVER BLOCKCHAIN

By

Al-ABADI HASSAN MANSUR HUSSIEN

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

December 2021

FSKTM 2021 15

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

TOWARD EFFICIENT ATTRIBUTE-BASED SEARCHABLE ENCRYPTION FOR ACCESS CONTROL OVER BLOCKCHAIN

By

Al-ABADI HASSAN MANSUR HUSSIEN

December 2021

Chair : Sharifah Md Yasin, PhD
Faculty : Computer Science and Information Technology

Blockchain technology offered a technical aspect that ultimately transforms the existing personal health record (PHR) systems into decentralised networks to decrease the possibility of a single point of security failure. However, such technology possesses some drawbacks, such as issues in privacy and storage capacity. By contrast, storing vast medical data significantly affects the repository storage of blockchain. This study bridges the gap between PHRs and blockchain by offloading the vast medical data into the InterPlanetary File System (IPFS) storage and establishing an enforced cryptographic authorisation and access control scheme searching on outsourced encrypted medical data. In the literature, the most promising solution technique to provide such a search on encrypted outsourced data is the searchable encryption schemes. Consequently, the advantages over the other searchable encryption scheme in the construction of secure, searchable fine-grained access control for outsourced encrypted data. However, the existing CP-ABSE schemes still ciphertext-policy attribute-based searchable encryption CP-ABSE has significant suffered from several issues. First, the key escrow in the trusted private key generator (PKG). Second, expensive computational operations in its data outsource and retrieval aspects. Third, secure conjunctive keyword search mechanisms. Fourth, support on-demand users and attribute revocation for dynamic policy updates. These concerns have not been addressed in the decentralised storage repository (IPFS) to exchange personal health records over the blockchain environment. This thesis aims to ensure patient data security by proposing a new two-fold fine-grained search access control policy for outsourcing encrypted medical data in normal and revocable situations.

This thesis proposed a new provable lightweight cryptographic concept named blockchain-based attribute-based searchable encryption BC-ABSE by extending ciphertext-policy attribute-based encryption (CP-ABE) and searchable symmetric encryption (SSE) and by leveraging the technology of smart contracts to achieve an effective and secure searchable access control scheme. The (BC-ABSE) cryptographic

concept is capable of achieving the following vital aspects: (1) Efficient and secure multikeyword searchable fine-grained access control of data over IPFS (2) Confidentiality of data by eliminating a trusted private key generator (PKG). Based on the decisional bilinear Diffie Hellman (DBDH) hardness assumptions and the discrete logarithm (DL) problems, the rigorous security analysis shows that the proposed scheme is secure against the chosen-keyword attack (SCKA) and keyword secrecy in the standard model. Besides, the user collusion attacks are prevented, and the tamper-proof resistance of data is ensured. Furthermore, security validation is verified by simulating a formal verification scenario using Automated Validation of Internet Security Protocols and Applications (AVISPA), thereby unveiling that BC-ABSE is resistant to man-in-the-middle (MIM) and replay attacks. The experimental analysis utilised real-world datasets to demonstrate the efficiency and utility of BC-ABSE in terms of computation overhead, storage cost, and communication overhead. The proposed scheme is also designed and developed to evaluate throughput and latency transactions using a standard benchmark tool known as Caliper. Lastly, simulation results show that BC-ABSE has high throughput and low latency, with an ultimate increase in network life compared with traditional healthcare systems

This thesis also proposed new efficient and secure user revocation and attributes policy update mechanism throughout BC-ABSE in the case of users revoking or upgrading their attributes in the system. Therefore, proxy re-encryption and lazy revocation are modelled on smart contracts to effectively revoke the attribute without needing an authentication centre and any additional communications between any authority. The security analysis shows that the indirect revocation model in BC-ABSE is able to prevent forward and backward attacks. The asymptotic complexity comparison and implementation results indicate that the proposed scheme can balance the security goals with practical computation efficiency. The proposed revocation mechanism simulation results on the blockchain network have high transaction throughput and guarantee reasonable transaction latency compared to the existing conventional revocation mechanism.

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

KE ARAH PENYULITAN BOLEH CARIAN BERASASKAN ATRIBUT YANG CEKAP UNTUK KAWALAN AKSES KE ATAS BLOCKCHAIN

Oleh

Al-ABADI HASSAN MANSUR HUSSIEN

Disember 2021

Pengerusi : Sharifah Md Yasin, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Teknologi blockchain menawarkan aspek teknikal yang akhirnya mengubah sistem rekod kesihatan peribadi (PHR) sedia ada kepada rangkaian terdesentralisasi untuk mengurangkan kemungkinan satu titik kegagalan keselamatan. Walau bagaimanapun, teknologi sedemikian mempunyai beberapa kelemahan, seperti isu dalam privasi dan kapasiti storan. Sebaliknya, menyimpan data perubatan yang luas sangat mempengaruhi penyimpanan repositori blockchain. Kajian ini merapatkan jurang antara PHR dan teknologi blockchain dengan memunggah data perubatan yang luas ke dalam storan Sistem Fail InterPlanetary (IPFS) dan mewujudkan kebenaran kriptografi yang dikuatkuasakan dan skim kawalan akses mencari pada data perubatan disulitkan luar. Dalam literatur, teknik penyelesaian yang paling menjanjikan untuk menyediakan carian sedemikian pada data penyumberan luar yang disulitkan ialah skim penyulitan yang boleh dicari. Akibatnya, penyulitan boleh carian berasaskan atribut teks-sifir CP-ABSE mempunyai kelebihan yang ketara berbanding skim penyulitan boleh carian lain dalam pembinaan kawalan capaian berbutir halus yang selamat dan boleh dicari untuk data disulitkan luar. Walau bagaimanapun, skim CP-ABSE sedia ada masih mengalami beberapa isu. Pertama, eskrow kunci dalam penjana kunci persendirian yang dipercayai (PKG). Kedua, operasi pengiraan yang mahal dalam aspek sumber luar dan pengambilan datanya. Ketiga, mekanisme carian kata kunci konjungtif yang selamat. Keempat, menyokong pengguna atas permintaan dan pembatalan atribut untuk kemas kini dasar dinamik. Kebimbangan ini belum ditangani dalam repositori storan terdesentralisasi (IPFS) untuk menukar rekod kesihatan peribadi melalui persekitaran blockchain. Tesis ini bertujuan untuk memastikan keselamatan data pesakit dengan mencadangkan dasar kawalan capaian carian terperinci dua kali ganda baharu untuk penyumberan luar data perubatan yang disulitkan dalam situasi biasa dan boleh dibatalkan.

Tesis ini mencadangkan konsep kriptografi ringan yang boleh dibuktikan baharu yang dinamakan penyulitan boleh carian berasaskan atribut berasaskan blokchain BC-ABSE dengan memperluaskan penyulitan berasaskan atribut dasar teks sifir (CP-ABE) dan

penyulitan simetri boleh carian (SSE) dan dengan memanfaatkan teknologi kontrak pintar. untuk mencapai skim kawalan capaian boleh carian yang berkesan dan selamat. Konsep kriptografi (BC-ABSE) mampu mencapai aspek penting berikut: (1) Kawalan capaian berbutir halus berbilang kata yang cekap dan selamat bagi data melalui IPFS (2) Kerahsiaan data dengan menghapuskan penjana kunci persendirian (PKG) yang dipercayai . Berdasarkan andaian kekerasan bilinear Diffie Hellman (DBDH) keputusan dan masalah logaritma diskret (DL), analisis keselamatan yang ketat menunjukkan bahawa skim yang dicadangkan selamat terhadap serangan kata kunci terpilih (SCKA) dan kerahsiaan kata kunci dalam model standard. Selain itu, serangan pakatan sulit pengguna dihalang, dan rintangan kalis gangguan data dipastikan. Tambahan pula, pengesahan keselamatan disahkan dengan mensimulasikan senario pengesahan rasmi menggunakan Pengesahan Automatik Protokol dan Aplikasi Keselamatan Internet (AVISPA), sekali gus mendedahkan bahawa BC-ABSE tahan terhadap serangan man-in-the-middle (MIM) dan main semula. Analisis percubaan menggunakan set data dunia sebenar untuk menunjukkan kecekapan dan utiliti BC-ABSE dari segi overhed pengiraan, kos penyimpanan dan overhed komunikasi. Skim yang dicadangkan juga direka bentuk dan dibangunkan untuk menilai transaksi daya pengeluaran dan kependaman menggunakan alat penanda aras standard yang dikenali sebagai Caliper. Akhir sekali, hasil simulasi menunjukkan bahawa BC-ABSE mempunyai daya pemprosesan yang tinggi dan kependaman rendah, dengan peningkatan muktamad dalam hayat rangkaian berbanding dengan sistem penjagaan kesihatan tradisional

Tesis ini juga mencadangkan mekanisme pengemaskinian dasar dan dasar pengemaskinian dasar pengguna yang cekap dan selamat di seluruh BC-ABSE sekiranya pengguna membatalkan atau menaik taraf atribut mereka dalam sistem. Oleh itu, penyulitan semula proksi dan pembatalan malas dimodelkan pada kontrak pintar untuk membatalkan atribut dengan berkesan tanpa memerlukan pusat pengesahan dan sebarang komunikasi tambahan antara mana-mana pihak berkuasa. Analisis keselamatan menunjukkan bahawa model pembatalan tidak langsung dalam BC-ABSE mampu mencegah serangan ke hadapan dan ke belakang. Perbandingan kerumitan asimptotik dan hasil pelaksanaan menunjukkan bahawa skim yang dicadangkan boleh mengimbangi matlamat keselamatan dengan kecekapan pengiraan praktikal. Keputusan simulasi mekanisme pembatalan yang dicadangkan pada rangkaian blockchain mempunyai daya pemprosesan transaksi yang tinggi dan menjamin kependaman transaksi yang munasabah berbanding dengan mekanisme pembatalan konvensional sedia ada

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest thankfulness and gratitude to the Almighty Allah for granting me this opportunity and for blessing this project.

I acknowledge my sincere appreciation and gratitude to my advisor of the study Dr. Sharifah Md. Yasin for her invaluable feedback on my research, for her support of my Ph.D., for her guidance and encouragement. I also would like to thank my university committee member Assoc. Prof Nur Izura binti Udzir and Dr Mohd Izuan bafez Bin Ninggal.

I cannot forget friends who went through hard times together, cheered me on, and celebrated each accomplishment: Haqi Khalid, Mustafa T. Al-samarie, Muntadher Saadoon, Sadeq Salman, hamza altarturi, Bahaa H. Almhanawi, Hussein Alsultan, Muntasser Al Anbagi, muath alali.

Most of all, I would like to express my deepest appreciation to my lovely family for their affectionate support, patience, and encouragement. Their prayers and good wishes constantly help me to be strong, especially in difficult times. I am forever grateful and indebted. To my late father, thank you for everything that you have given to me. You are proud of me; I know it. To my brothers, Majid, Khaled, and sisters Meadia, Muna, Marwa, Maryam, thank you for your heart-warming kindness and support. And finally, the one person who has made this all possible has been my mum Amirah Farman. She has been a constant source of support and encouragement and has made an untold number of sacrifices for the entire family, and specifically for me to continue my schooling. She is a great inspiration to me. Hence, great appreciation and enormous thanks are due to her, for without her understanding, I am sure this thesis would never have been completed without her prayers. I also would like to express my gratitude to my brothers-in-law Haider, Mustafa, and Ahmed for their unfailing emotional support. I also thank my sisters-in-law Asma and Zahraa for their kind support. I thank you all.

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:

Sharifah binti Md. Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Nur Izura binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohd Izuan Hafez bin Ninggal, PhD
Senior Lecturer
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: 19 May 2022

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

5G	Fifth-generation mobile network technology
AES	Advanced Encryption Standard
AI	Artificial intelligence
AVISPA	Automated Validation of Internet Security Protocols and Applications
BC	Blockchain
CA	central authority
CP-ABSE	ciphertext-policy attribute-based searchable encryption
DBDH	decisional bilinear Diffie Hellman
DL	discrete logarithm
EEG	Electroencephalography
EHRs	Electronic health records’
EMR	Electronic Medical records’
FHIR	Fast Healthcare Interoperability Resources
HL7	Health Level Seven International
HUN	Healthcare Users Node
IHE	Integrating the Healthcare Enterprise
IoMT	Internet of Medical Things
IoT	Internet of Things
IPFS	InterPlanetary File System
KP-ABSE	key-policy attribute-based searchable encryption
KS	keyword secrecy
PBFT	Practical Byzantine fault tolerance

PEKS	Public-key encryption with keyword search
PEKS	Public key encryption with keyword search
PHRs	Personal health records
PKG	trusted private key generator
PN	Patient Node
PoA	Proof of authority
PoS	Proof of stake
PoW	Proof of work
PSN	Pervasive social network
PPT	probabilistic polynomial-time
RESTful API	Representational state transfer
RPM	Remote patient monitoring
RSA	Rivest–Shamir–Adleman public-key cryptosystem
BC-ABSE	Blockchain-based attribute-based searchable encryption
SCKA	chosen-keyword attack
SSE	searchable symmetric encryption
TMIS	Telecare medical information systems

CHAPTER 1

INTRODUCTION

The potential of blockchain technology provides a tremendous advantage to transform the current infrastructure systems into decentralised networks due to its unique concepts such as immutability, cryptography, consistency, consensus protocols, and smart contracts. This thesis focused on the Ethereum blockchain platform to develop a secure access control scheme for sharing personal health records. Ethereum blockchain is considered an unpermissioned ledger when nodes interconnected to the network are accessible to anyone via the Internet. Accordingly, any network member can validate a transaction and participate in the approval process through the consensus algorithm, such as proof of work or proof of authority. A blockchain is primarily designed to securely eliminate centralised authority in a digital asset scenario exchange. A block of chains is established in P2P transactions to ensure decentralisation. Each transaction is linked to the previous transaction through the cryptographic hash Merkle tree as a block of the chains prior to being entered into the immutable database of the system. Therefore, the blockchain transaction ledger is compatible and synchronisation with every node in the network. Anyone with a computer and Internet connection will be allowed to register as a node and be offered a complete blockchain record. The repetition of synchronised public blockchains with each node in the network makes the system completely secure. In recent years, the combination of Ethereum blockchain with PHR together has emerged as a preferable platform for developing trustworthy distributed medical applications. This new unique computing paradigm raises new challenges in terms of security and privacy. These concerns arise from the lack of a secure access control system to avoid data interference with confidential data to the general public on blockchain networks. However, the large scale distributed nature of medical databases requires limited computational and storage capabilities. The traditional access control schemes are not immediately applicable due to the unique paradigm and properties of the PHR-based blockchain.

The sharing of personal health records (PHRs) is vital for diagnosis and disease care to facilitate patients' treatment by various medical professionals. PHR systems have become the standard technology that handles the proliferation of generated medical records whilst maintaining the required quality of services. Furthermore, potential blockchain technology enablers, such as decentralised networks, transactions, consensus mechanisms and smart contracts, can improve security and integrity. However, issues that concern private blockchain such as Ethereum is related to privacy and storage capacity. The development of PHR applications on the Ethereum blockchain network may enable anyone to access transaction data due to the blockchain's transparent feature. This feature has raised privacy concerns regarding HIPAA requirements and the ability of patients to participate in the publication of their personal information in the Ethereum blockchain network. By contrast, Ethereum blockchain requires considerable storage to record whole transactions in the network; such requirement can be a problem for restrictive nodes that send data to the network. Ethereum Blockchain can ensure that the stored and shared PHRs are not manipulated, unforgeable and verifiable but can effectively suffer from storage requirements of large-scale distributed data. Recent

findings tend to resolve the above issues by storing medical databases on offline storage, such as cloud servers, and by setting up an access control scheme to prevent unauthorised users from manipulating data through leveraging the attribute-based cryptosystem reproxy encryption and smart contracts to control the users' privilege. At the same time, other researchers have attempted to offload the actual large-scale distributed data into the InterPlanetary File System (IPFS) storage without setting up any enforced cryptographic access control. Consequently, the outsourcing of databases on IPFS decentralised storage eliminates the unreliable storage of third parties. Nevertheless, IPFS has a noticeable security flow that anyone with the hash of the file stored therein can easily retrieve it due to IPFS native workflow. In conclusion, the health data generated by patients are not well suitable for being stored in IPFS unless data are encrypted individually prior to outsourcing to the IPFS. Therefore, providing security and privacy to PHR systems with fine-grained access control is essential to support a technique that searches for encrypted data on the IPFS storage.

In this chapter, Sections 1.1 presents the background. The research motivation presents in section 1.2. The research problem, research questions, research objectives, research scope and the contributions of this thesis are introduced in Sections 1.3, 1.5, 1.5, 1.6 and 1.7, respectively. The outline of the thesis organisation is presented in Section 1.8.

1.1 Background

Health care is a vital area of information technology (IT) because this sector has substantially evolved through personal health records (PHR), remote patient monitoring (RPM), and population health management tools. The medical data generated from these sources are vast and cumbersome, thereby leading to problems with the quality of medical data, such as complicated analysis, diagnosis, and prediction, and data confidentiality risk due to the increasing number of cybercrime cases (Schwartz et al., 2012). The personal health records system (PHR) has proven its importance to patients because of the valuable asset recorded in consonance with their point of view. Although sharing patient information amongst various healthcare providers through the system may boost diagnostic accuracy, the health information repository may become a single point of security failure. It may be targeted by attackers resulting in ransomware attacks or denial of services (Rezaeibagha et al., 2015). Therefore, data security is an important component of healthcare applications and plays a crucial role in protecting sensitive data. Healthcare data include patient details, which should not be disclosed to any untrusted third-party because of safety issues and information misuse. This type of data comprises a list of patient information in medical repositories gathered from the beginning of patient illness to recovery. Such data also include a series of time-bound information recorded by hospitals (see Figure 1.1). However, healthcare data or clinical information are spread amongst different medical repositories. Consequently, this feature may lead to the disclosure of patients' data. It may not fulfil the legal requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Abouelmehdi et al., 2018). However, sharing and accessing medical records in the PHR system is extremely significant for receiving intelligent and advanced medical services (Alonso et al., 2019).

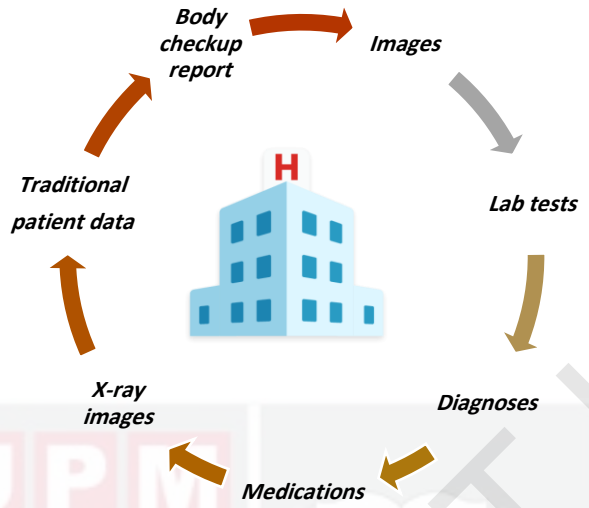

Figure 1.1 : Personal health record cycle (Bennett, 2018)

Emerging technological breakthroughs in blockchain and smart contracts are expected to provide promising solutions to secure patient data despite being shared and accessed through multiple healthcare providers. The concepts of shared health information exchange (HIE) rely on blockchain technology is to remove restrictions that separate independent healthcare providers and make personal health records universal and shareable. The integration of the blockchain technology into the application of personal health records (PHRs) application content of three layers, as shown in Figure 1.2.

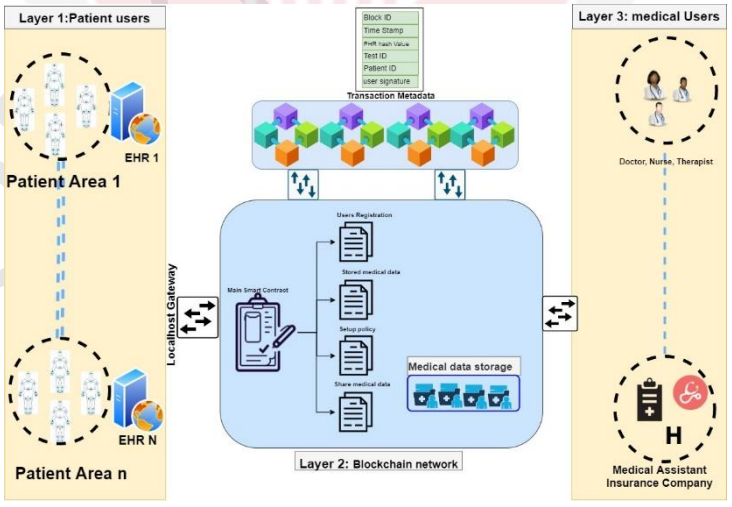

Figure 1.2: General architecture of blockchain in sharing of personal health (Bennett, 2018)

The patient users' layer is a group of patients connected to the sensors to monitor their health conditions for diagnostic purposes, such as surgery, hospital visits, and monitoring of elderly patients at home. The blockchain network layer is responsible for storing, sharing, updating the healthcare players' entities. The medical users are a group of health professionals, such as physicians, hospitals, health insurance, medical organisations, who seek better and more accessible treatment for patients using the blockchain network. This integration provides meaningful contributions to human health and wellbeing. Evidently, smart contracts can approve multiple signatures amongst patients and healthcare providers, thereby allowing only authorised users or devices to access or attach recorded data in the system. This feature ensures that patients can verify the authenticity of the data recorded in the system whilst maintaining the anonymity of their real identity. Smart contracts also enable interoperability through collaborative version control to maintain record consistency. Additionally, smart contracts can provide researchers with access to personal health information (PHI) and enable automatic micropayments to benefit patients and healthcare providers involved in the blockchain network. However, issues that concern blockchain or smart contract are related to security, privacy and storage capacity (Feng et al., 2018; X. Li et al., 2017; Yli-Huumo et al., 2016). The development of personal health records (PHR) applications on the blockchain network may enable anyone to access transaction data due to the blockchain's transparent feature. This feature has raised privacy concerns regarding HIPAA requirements and the ability of patients' participation to publish their personal information in the public blockchain network (Bennett, 2018). On the other side, the blockchain requires significant storage to record whole transactions in the network, which can be a problem for restrictive nodes that send data to the network. Blockchain can ensure that the stored and shared personal health records are not manipulated, unforgeable, and verifiable but can effectively suffer from large-scale distributed data storage requirements (Rouhani, 2019; Sun et al., 2018).

A significant detail to be considered is to examine the advantages and disadvantages of using blockchain technology for PHR against a range of perspectives, such as security, privacy, and storage capacity. The latest findings tend to resolve the issues mentioned above by storing the medical databases on offline storage such as cloud server and setting up an access control scheme to preventing unauthorised users from manipulating data by leveraging the attributes-based cryptosystem (Iqbal et al., 2019; Pournaghi et al., 2020),re-proxy encryption (Hylock & Zeng 2019; Thwin & Vasupongayya 2019) and smart contracts (Khatoon, 2020; Hui Li et al., 2018; Xia et al., 2017; Yongbin Zhang et al., 2019) to control the users' privilege. At the same time, other researchers attempt to offload the actual large-scale distributed data into the InterPlanetary File System (IPFS) storage without setup any enforced cryptographic access control (Naz et al., 2019; Steichen et al., 2018). Meanwhile, the idea beyond the outsourced blockchain database on cloud storage addresses the scalability problem. However, it decreases the extent of protection of blockchain toward a single point of security failure.

Cryptographic primitives' methods are considered to be the appropriate solution for the confidentiality of data. However, traditional cryptographic primitives' methods, such as symmetric-key encryption and public-key encryption, are unable to maintain effective access control over encrypted data. The ciphertext-policy attribute-based searchable encryption (CP-ABSE) has significant advantages over the other encryption scheme in constructing secure, searchable fine-grained access control for outsourced encrypted

data. The CP-ABSE is a suitable scheme for storing medical data in the IPFS node by enabling fine-grained access control in an encrypted electronic format to control user privilege and support one-to-many scenarios. This scheme is capable of supporting expressive access policies by determining any access structures. This scheme also provides a high data flexibility level because the data consumers' secret keys can be generated at once and can be used to decrypt all the reverent ciphertext.

1.2 Motivation

The emergence of PHR sharing systems using cloud technology can provide patients with a complete and accurate online personal medical history, which can benefit patients, research institutions, pharmaceutical companies, and the entire healthcare system. Under these circumstances, the patient's PHRs are often outsourced to a third party, such as the cloud service provider, to achieve resource sharing and reduce the data centre's maintenance costs. This situation leads to security issues on how to ensure the security, privacy and searchability of PHRs. To overcome this problem, some researchers are attempting to combine searchable symmetric encryption and ciphertext-policy attribute-based encryption. However, this hybrid encryption scheme requires centralised key management in a cloud server, leading to a single point of security failure because the cloud platform may not be credible due to employee corruption or a threat to the authorisation centre. Fortunately, the use of blockchain technology and smart contracts can easily and securely manage key management and distribution. The concept of creating a permanent and decentralised way to store and share files on IPFS can be perfectly aligned with the blockchain for the provision of a decentralisation infrastructure. Additional blockchain features, such as unforgeable and tamper-proofing of stored data, are also an advantage.

1.3 Research Problems

The traditional (CP-ABSE) encryption schemes require a key generation centre (KGC) acting as a third-party authority to initialise and distribute a secret key to users. The PKG may cause serious issues with user data ownership, such as key misuse and data leakage. The data ownership cannot control their data due to PKG's ability to decrypt all outsourced data stored on the server. Meanwhile, the current (CP-ABSE) scheme has been suffered by expensive computational operations in its data outsourcing and retrieval aspects. While the current SSE schemes require crucial and costly key distribution and cannot support one-to-many encryption. SSE schemes use a single keyword to check all encrypted files and compare these files to the searched keyword to see whether the keyword is present in the scanned files. However, it is inefficient, particularly when the data size is massive, and it is only secure against a chosen-plaintext attack (CPA). SSE is an inefficient performance by high computational complexity that burdens user experience due to expensive pairing operations , (Alderman, Martin, & Renwick, 2017; Emura, Ito, & Ohigashi, 2020; C. Liu, Zhu, & Chen, 2017). SSE is impractical since data is often updated, even when stored on a remote server. The server cannot update the encrypted data without decrypting it. When the consumer who searches through the data is also the one who produces it, this configuration is insufficient. Nevertheless, it lacks

functionality since it can only be used with a single user scenario. Furthermore, the access patterns are leaked by the majority of SSE schemes , (Sheng Cao, Zhang, Liu, Zhang, & Neri, 2019; L. Chen, Lee, Chang, Choo, & Zhang, 2019; Yi Chen, Ding, Xu, Zheng, & Yang, 2018).

The personal health records (PHRs) system based on the cloud server is unreliable. This is due to the weakness of centralised systems. It is incapable of protecting both the confidentiality and integrity of users' sensitive information in uploading and sharing patient data among multiple health providers (Jin et al., 2019). In recent years, the blockchain technology has considerable attention in many industrial and academia aspects. In the healthcare industry, the blockchain has played a significant role in transforming the network infrastructure into a stable, auditable, and decentralised environment (Abu-elezz et al., 2020; Hasselgren et al., 2020). However, there are some technical barriers facing blockchains platforms, such as restricted storage and privacy concerns (de Haro-Olmo et al., 2020; Sharma et al., 2020). In the literature, the most promising solution to the above problems is to set up an access control scheme based on ciphertext-policy attribute-based searchable encryption (CP-ABSE) to outsource the medical data on the offline server storage such as cloud computing, or IFPS. The concepts of outsourced storage of the blockchain database on honest-but-curious third-party storage, such as cloud servers, are considered a double-edged sword technique that resolves the scalability storage issue but reduces the level of security of blockchain against fully decentralised infrastructure. At the same time, the IPFS decentralised storage is required the medical data to be encrypted individually prior to outsourcing therein. On the other side, the ciphertext-policy attribute-based searchable encryption (CP-ABSE) cryptographic primitive is an effective and appealing technique to provide a strict access policy for outsourced encrypted data. The CP-ABSE scheme permits the data owner to set attributes for their data. Search control policies can encrypt it prior to outsourced encrypted data to the server. Despite the notable significance of the existing CP-ABSE schemes, limitations are still observed in maintaining the desired security resistance, expensive computational operations, and capabilities to support users' revocation. Specifically, this thesis considered the above issues towards integration with blockchain and personal health records (PHR) system together over IPFS decentralised storage by addressing the following drawbacks:

- The first challenge of the current CP-ABSE that impedes its usability in certain practical applications, such as personal health records (PHRs), is the central authority (CA) known as the key generation centre (KGC). This centre is responsible for generating private keys for users by adding KGC master secret keys to the corresponding users' attribute set. The downside of KGC is a key escrow problem in which the curious KGC has the ability to decrypt the ciphertext stored in the server (Yang Chen, Wen, Li, Zhang, & Jin, 2018; Hur, Koo, Hwang, & Kang, 2013; Lin, Hong, & Sun, 2017; Sultan, Barbhuiya, & Sarma, 2017). This process violates users' privacy and degrades the security level of outsourcing encrypted over IPFS storage and may not fulfil the data owners' right for their sensitive PHRs to be decrypted by only authorised entities with specified attributes. The single-keyword search in CP-ABSE is a trivial procedure by performing each keyword separately resulted in inefficient queries and leaked some information to the server. While the multi-keywords keyword search allows a user to obtain encrypted data over the sever by attached several

keywords during one single query. Moreover, the design of a secure multi-keywords searchable mechanism without compromising the security resistance against chosen keyword attack, and keyword secrecy, in the standard model under the decisional bilinear Diffie Hellman (DBDH) hardness assumption remains to be challenged task (Bösch, Hartel, Jonker, & Peter, 2014; R. Zhang, Xue, & Liu, 2018; Zhou, Li, Tian, An, & Wang, 2020).

- The second challenge faced by CP-ABSE is an inefficient performance by high computational complexity that burdens user experience in key generation, token generation, data outsourcing, and data retrieval due to expensive pairing operations (Belguith, Kaaniche, & Hammoudeh, 2019; Pirretti, Traynor, Mcdaniel, & Waters, 2010; Yinghui Zhang et al., 2020; Q. Zheng, Xu, & Ateniese, 2014). The vast number of pairing operations employed in CP-ABSE is the main cause of its low-performance efficiency. This high computation can be a bottleneck for the users to upload and share medical data over an IPFS storage in a blockchain environment.

- The third challenge is revocation mechanism for CP-ABSE schemes that delegate honest-but-curious third-party servers such as a proxy server to conduct the revocation and attribute revocation for the re-encrypted ciphertext and re-generate a new secret key respectively. However, the reliance on untrusted servers to perform this update is a drawback of these schemes (Al-Dahhan et al., 2019; Edemacu et al., 2019; P, P, & P.J.A., 2018). This process violates the privacy of the medical data stored in IPFS because the proxy server is capable of exposing the sensitive information of users (J. Sun et al., 2020). Moreover, the security issues that hinder the existing revocation are forward and backward attacks. In the case of a forward attack, the users who have been revoked from the system should not be able to access the subsequent ciphertext stored in the IPFS storage over blockchain environment by using their old version of the secret key. In the case of backward attacks, the newly joined user into the system should access the previously stored ciphertext in IPFS storage over blockchain environment if and only if the new user attribute set has been satisfied with the access policy embedded into ciphertext.

1.4 Research Questions

This thesis proposes an enhancement to the security of the ciphertext-policy attribute-based encryption with a keyword search by redesigning the scheme to be support user access control for sharing personal health records over the blockchain. As a result, the thesis' main outcomes can be concluded as the following formulation research questions

(1). How to design secure ciphertext-policy attribute-based encryption with keyword search scheme to support a multi-keyword searchable fine-grained access control for sharing personal health records in blockchain over IPFS?

(2). How to ensure the proposed scheme achieves a higher level of security with less computational complexity costs than other existing state-of-the-art schemes?

(3). How to design a secure user revocation and attributes revocation without compromising users' privacy and reducing the computation costs?

1.5 Research Objectives

This research generally aims to design a new two-fold secure multikeywords searchable access control mechanism based on the attribute-based encryption schemes in normal and revocable situations over blockchain-based personal health records (PHR) system. This enables the patient users to store and share their medical records in a decentralised storage repository (IPFS) while preventing unauthorised users from disclosing medical data. In details, this can be described throughout the following objective:

1) To propose a new provable secure cryptographic primitive named blockchain attribute-based searchable encryption (BC-ABSE) by extending ciphertext-policy attribute-based encryption (CP-ABE) and searchable symmetric encryption (SSE) and by leveraging the technology of smart contracts for designing secure access control scheme for sharing personal health records over decentralised IPFS storage.

2) To propose a new mechanism that minimises the high pairing complexity to reduce the user's computation burden in key generation, data outsourcing, token generation, and data retrieval in CP-ABSE schemes.

3) To propose a secure user and attributes revocations mechanism throughout BC-ABSE by leveraging re-encryption and lazy revocation technique without relying on the proxy server.

1.6 Research Scope

This thesis mainly concentrates on the access and store of medical data in IPFS decentralised storage over the blockchain environment under the scenario of personal health records systems to ensure security and privacy. The main concern of this research is the most promising solution to develop an access control scheme based on ciphertext-policy attribute-based searchable encryption (CP-ABSE) where enhancements are made by proposing a new lightweight cryptographic primitive. The newly proposed cryptographic primitive BC-ABSE enables the patient-user to outsource the encrypted medical data on the storage of IFPS under a defined set of attributes by formulating search control policies. Moreover, only the data user consumer who attributes satisfy the access policy can decrypt the medial data. Figure 1.3 conceives an evident and comprehensive description of the research scope. Besides, the proposed scheme revisited and resolved the issues associated with conventional approaches CP-ABSE in the design of an efficient and secure, multikeyword searchable fine-grained access control, and realised on-demand user attribute revocation, and policy update.

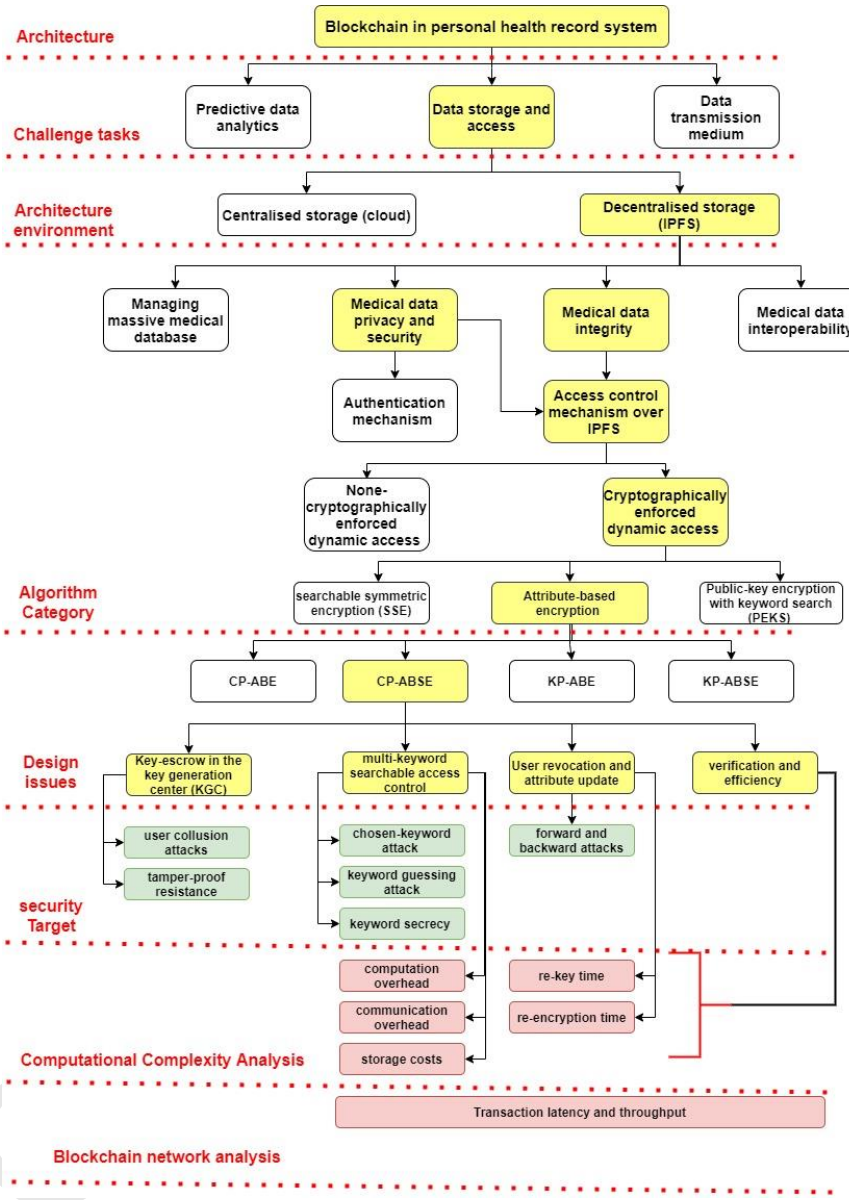

Figure 1.3 : Thesis research scope

This thesis proposed a new lightweight cryptographic concept called blockchain attribute-based searchable encryption BC-ABSE through combining CP-ABE, SSE, smart contract, and IPFS storage. The proposed scheme BC-ABSE eliminates the need for a key generation centre (KGC) from the system by allowing the data owner to distribute secret keys to data users in order to control their outsourced encrypted data stored in IPFS, which would be more effective than the traditional CP-ABSE schemes. At the same time, the smart contract in the blockchain is being used to maintain the secret

key of users, and the problem of key management in the traditional CP-ABE schemes has been resolved. The proposed scheme (BC-ABSE) has supported the user's revocation using proxy re-encryption technique in the decentralised blockchain environment over IPFS that does not require a central authority. This scheme also addressed the burden of computation complexity users by requiring less communication and computation costs due to the use of few pairing operations. This new BC-ABSE scheme solves the current problems of developing personal health records (PHR) application based on blockchain technology by designing new two-fold a secure and efficient authorisation and access control mechanism for normal and revocable situations to allow patients to store and share their medical record in a decentralised storage repository (IPFS) while preventing unauthorised users from disclosing medical data.

1.7 Research Contributions

The significant contribution of this research is an improvement towards the CP-ABSE to strengthen its capabilities in aspects of security and efficiency. It also expands its functionality of supporting multi keyword searchable mechanisms and user revocation to be more suitable cryptographic primitives for blockchain-based personal health records (PHR) systems over IPFS decentralised storage. Therefore, this thesis has been proposed a new cryptographic concept named Blockchain Attribute-based searchable Encryption (BC-ABSE) to support regular and revocable user's access control. The main contributions of the thesis are as subsequent:

- Scheme BC-ABSE removed central authority (CA) by achieves high privacy protection of users to generate a secret key. This study addresses the drawbacks of all single authority systems and some multi-authority schemes in aspects of single points of security failure. In addition, there is no such entity that has complete control over all data in scheme. This respective solution resolves the shortcomings of the most relevant schemes of ABE works by enhancing the degree of data privacy. The proposed scheme BC-ABSE supports secure multikeyword searchable fine-grained access control to remedy the trivial current method to handle a wide range of searchable attributes on outsourced encrypted data medical data over IPFS decentralised storage. The proposed scheme BC-ABSE is proven to be secure against chosen-keyword attack (SCKA), and keyword secrecy (KS) under the hardness assumptions of DBDH and DL problems, respectively, in the standard model. In addition, the semantic security proof indicted that the user collusion attacks are prevented, and the tamper-proof resistance of data is ensured. Moreover, the formal security verification method using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool verifies that the reinforced security validation of the proposed scheme withstands replay and MITM attacks.

- The lightweight key generation algorithm is proposed in the BC-ABSE scheme in comparison with other existing schemes due to reducing the number of pairing operations in which it is a more constant secret key. A lightweight encryption algorithm was proposed in data outsourcing by implementing symmetric key encryption (AES) to turn into constant ciphertext. In aspects of the data retrieving, a lightweight token generation algorithm was proposed by

shifting almost all of the pairing operations' computational complexity processes to the search part of the IPFS storage entity. Generally, the encryption and decryption of the medical data do not depend on the number of attributes in the access control policies.

- The mechanism in BC-ABSE allows on-demand user/attribute revocation due to use the lazy re-encryption algorithm without relying upon the proxy server. The proposed scheme uses the re-key generation algorithm to allow a data owner to use a re-encryption key to convert encryption under one key into encryption under the other key of the same message. Also, when only necessary, the lazy re-encryption was used to update medical data stored on IPFS. The proposed scheme of user revocation and attribute policy update in terms of re-key secret key generation has a lower computation complexity than relevant schemes due to fewer pairing operations and only one exponential operation of element group required. In comparison, the proposed scheme for updating stored medical data in decentralised storage IPFS of re-encryption only requires updating the symmetric key encryption (SKE) and keywords file index with a new access policy for the number of leaf nodes used. The proposed scheme of user revocation and attribute policy in BC-ABSE insured the forward and backward secrecy. In addition, the semantic security proof indicted that the user collusion attacks are prevented, and the tamper-proof resistance of data is ensured.

1.8 Thesis Organisation

This rest outline thesis is organised as follows:

Chapter 2- presents the literature review. It started with a brief introduction to blockchain technology by determining the main components within its innovation characteristic. A general evaluation framework has been discussed to determine the use of blockchain in the personal health records system. Besides, potentials and its challenges of attribute-based searchable encryption in blockchain-based personal health records have been thoroughly discussed. The related works of designed issues in the security, efficiency, expand its functionality of supporting searchable mechanism, and user revocation are discussed and analysed accordingly
.

Chapter 3 - provides a brief explanation of the research methodology adopted in this research. The requirement analysis for this research is discussed, and the design smart contract attribute-based searchable encryption BC-ABSE. The implementation stages are shown in detail and experimental evaluation in terms of security and efficiency and analysis of the proposed scheme are also highlighted.

Chapter 4 - proposed a searchable encryption scheme for blockchain, namely smart contract Attribute-based Searchable Encryption BC-ABSE, to develop an access control for shared personal health records over decentralised storage. The security and performance analyses of the proposed scheme are provided.

Chapter 5 - presents a secure mechanism for user revocation with a revocation attributes policy mechanism for BC-ABSE. The security analysis proof against forward and backward attacks is discussed and analysed accordingly. The performance analysis of the revocation mechanism has been demonstrating with respect to relevant benchmarking schemes.

Chapter 6 - summarises the entire thesis and provides recommendations on possible extensions or future work for this research.

REFERENCES

Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., … Shi, H. (2008). Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. *Journal of Cryptology*, *21*(3), 350–391. https://doi.org/10.1007/s00145-007-9006-6.

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1), 1. https://doi.org/10.1186/s40537-017-0110-7.

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73–80. https://doi.org/10.1016/j.procs.2017.08.292.

Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, *142*(February), 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246.

Al-Dahhan, R. R., Shi, Q., Lee, G. M., & Kifayat, K. (2019). Survey on revocation in ciphertext-policy attribute-based encryption. *Sensors (Switzerland)*, *19*(7), 1–22. https://doi.org/10.3390/s19071695.

Alderman, J., Martin, K. M., & Renwick, S. L. (2017). Multi-level access in searchable symmetric encryption. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10323 LNCS*, 35–52. https://doi.org/10.1007/978-3-319-70278-0_3.

Ali, M., & Sadeghi, M. R. (2020). Provable secure lightweight attribute-based keyword search for cloud-based Internet of Things networks. *Transactions on Emerging Telecommunications Technologies*, (December 2019), 1–19. https://doi.org/10.1002/ett.3905.

Alonso, S. G., Arambarri, J., López-Coronado, M., & de la Torre Díez, I. (2019). Proposing New Blockchain Challenges in eHealth. *Journal of Medical Systems*. Journal of Medical Systems. https://doi.org/10.1007/s10916-019-1195-7.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., … Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *ArXiv*. https://doi.org/10.1145/3190508.3190538.

Anoaica, A., & Levard, H. (2018). Quantitative Description of Internal Activity on the Ethereum Public Blockchain. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1–5. https://doi.org/10.1109/NTMS.2018.8328741.

Armando, A., Basin, D., Boichut, Y., Chevalier, Y., & Compagna, L. (2005). The AVISPA Tool for the Automated Validation. *Computer Aided Verification*, *3576*,

281–285.

Ateniese, G., Fu, K., Green, M., & Hohenberger, S. (2006). Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security*, *9*(1), 1–30. https://doi.org/10.1145/1127345.1127346.

Attrapadung, N., Libert, B., & de Panafieu, E. (2011). Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts (pp. 90–108). https://doi.org/10.1007/978-3-642-19379-8_6.

Baek, J., Safavi-Naini, R., & Susilo, W. (2008). Public key encryption with keyword search. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5072 LNCS*(PART 1), 1249–1259. https://doi.org/10.1007/978-3-540-69839-5_96.

Bak, S., Pyo, Y., & Jeong, J. (2019). Protection of EEG Data using Blockchain Platform. In *7th International Winter Conference on Brain-Computer Interface, BCI 2019*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/IWW-BCI.2019.8737260.

Balu, A., & Kuppusamy, K. (2014). An expressive and provably secure Ciphertext-Policy Attribute-Based Encryption. *Information Sciences*, *276*(subaward 641), 354–362. https://doi.org/10.1016/j.ins.2013.12.027.

Belguith, S., Kaaniche, N., & Hammoudeh, M. (2019). Analysis of attribute-based cryptographic techniques and their application to protect cloud services. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.3667.

Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System, (Draft 3). Retrieved from http://arxiv.org/abs/1407.3561.

Benil, T., & Jasper, J. (2020). Cloud based security on outsourcing using blockchain in E-health systems. *Computer Networks*, *178*(December 2019), 107344. https://doi.org/10.1016/j.comnet.2020.107344.

Bennett, B. (2018). Blockchain HIE Overview: A Framework for Healthcare Interoperability. *Telehealth and Medicine Today*, *2*(3), 1–6. https://doi.org/10.30953/tmt.v2.14.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. *Proceedings - IEEE Symposium on Security and Privacy*, 321–334. https://doi.org/10.1109/SP.2007.11.

Bonneau, J., Eds, N. H., & Goos, G. (2020). *Financial Cryptography and Data Security*. https://doi.org/10.1007/978-3-030-51280-4.

Bösch, C., Hartel, P., Jonker, W., & Peter, A. (2014). A survey of provably secure searchable encryption. *ACM Computing Surveys*, *47*(2).

https://doi.org/10.1145/2636328.

Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2014). Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems*, *25*(1), 222–233. https://doi.org/10.1109/TPDS.2013.45.

Cao, S, Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences*, *485*, 427–440. https://doi.org/10.1016/j.ins.2019.02.038.

Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance, (February), 1–14.

Chase, B., & MacBrough, E. (2018). Analysis of the XRP Ledger Consensus Protocol. *A*. Retrieved from http://arxiv.org/abs/1802.07242.

Chatterjee, S., & Das, A. K. (2015). An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Security and Communication Networks*, *8*(9), 1752–1771. https://doi.org/10.1002/sec.1140.

Chen, C. L., Deng, Y. Y., Weng, W., Sun, H., & Zhou, M. (2020). A blockchain-based secure inter-hospital EMR sharing system. *Applied Sciences (Switzerland)*, *10*(14). https://doi.org/10.3390/app10144958.

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE*, *95*, 420–429. https://doi.org/10.1016/j.future.2019.01.018.

Chen, Yang, Wen, Q., Li, W., Zhang, H., & Jin, Z. (2018). Generic construction of outsourced attribute-based encryption without key escrow. *IEEE Access*, *6*, 58955–58966. https://doi.org/10.1109/ACCESS.2018.2875070.

Chen, Yi, Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *Journal of Medical Systems*, *43*(1). https://doi.org/10.1007/s10916-018-1121-4.

Chen, Yong. (2020). A Review of Research Relevant to the Emerging Industry Trends: Industry 4.0, IoT, Blockchain, and Business Analytics, *5*(1), 1–16. https://doi.org/10.1142/S2424862219500192.

Christoph, B., Tang, Q., Hartel, P., & Jonker, W. (2012). from Encrypted Database. *Springer Berlin Heidelberg*, 224–241. Retrieved from https://doi.org/10.1007/978-3-642-33383-5_14%0A.

Coelho, I. M., Coelho, V. N., Araujo, R. P., Yong Qiang, W., & Rhodes, B. D. (2020). Challenges of pbft-inspired consensus for blockchain and enhancements over neo dbft. Future Internet, 12(8), 129.

Cui, J., Zhou, H., Zhong, H., & Xu, Y. (2018). AKSER: Attribute-based keyword search with efficient revocation in cloud computing. *Information Sciences*, *423*, 343–352. https://doi.org/10.1016/j.ins.2017.09.029.

Curtmola, R., & Garay, J. (2011). Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. *Proceedings of the 13th …*, 1–33. Retrieved from http://dl.acm.org/citation.cfm?id=1180417.

Daraghmi, E.-Y., Daraghmi, Y.-A., & Yuan, S.-M. (2019). MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access*, *7*, 164595–164613. https://doi.org/10.1109/ACCESS.2019.2952942

de Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. *Sensors*, *20*(24), 7171. https://doi.org/10.3390/s20247171.

Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access*, *7*(8), 38431–38441. https://doi.org/10.1109/ACCESS.2019.2905846.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, *30*(7), 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227.

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., … Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*, *22*(8), 1–15. https://doi.org/10.2196/13598.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *SENSORS*, *19*(2). https://doi.org/10.3390/s19020326.

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. https://doi.org/10.1109/ACCESS.2019.2925390.

Emura, K., Ito, K., & Ohigashi, T. (2020). Secure-channel free searchable encryption with multiple keywords: A generic construction, an instantiation, and its implementation. *Journal of Computer and System Sciences*, *114*, 107–125. https://doi.org/10.1016/j.jcss.2020.06.003.

Feng, L., & Zhang, H. (2018). System architecture for high-performance permissioned blockchains. *Frontiers of Computer Science*, 1–15. https://doi.org/https://doi.org/10.1007/s11704-018-6345-4.

Feng, Q., He, D., Zeadally, S., Khurram, M., & Kumar, N. (2018). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications.*

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: a systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2019). A Review on the Application of Blockchain for the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access*, *7*, 45201–45218. Retrieved from http://arxiv.org/abs/1902.09604.

Founder, G. W., & Gavin, E. (2014). *Ethereum: a secure decentralised generalised transaction ledger*. *Ethereum project yellow paper*.

Fu, J., Wang, N., & Cai, Y. (2020). Privacy-preserving in healthcare blockchain systems based on lightweight message sharing. *Sensors (Switzerland)*, *20*(7), 1–16. https://doi.org/10.3390/s20071898.

Gan, C., Saini, A., Zhu, Q., Xiang, Y., & Zhang, Z. (2020). Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-020-09322-6.

Gao, Z., Xu, L., Chen, L., Zhao, X., Lu, Y., & Shi, W. (2018). CoC: A Unified Distributed Ledger Based Supply Chain Management System. *Journal of Computer Science and Technology*, *33*(2), 237–248. https://doi.org/10.1007/s11390-018-1816-5.

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. *Journal of Management Analytics*, *7*(3), 321–343. https://doi.org/10.1080/23270012.2020.1801529.

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the ACM Conference on Computer and Communications Security*, 89–98. https://doi.org/10.1145/1180405.1180418.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, *42*(7), 1–7. https://doi.org/10.1007/s10916-018-0982-x.

Gudeme, J. R., Pasupuleti, S. K., & Kandukuri, R. (2021). Attribute-based public integrity auditing for shared data with efficient user revocation in cloud storage. *Journal of Ambient Intelligence and Humanized Computing*, *12*(2), 2019–2032. https://doi.org/10.1007/s12652-020-02302-6.

Guo, R., Shi, H., Zheng, D., Jing, C., Zhuang, C., & Wang, Z. (2019). Flexible and Efficient Blockchain-Based ABE Scheme with Multi-Authority for Medical on Demand in Telemedicine System. *IEEE Access*, *7*, 88012–88025. https://doi.org/10.1109/ACCESS.2019.2925625.

Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Sadoun, B. (2019). HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0. *CITS 2019 - Proceeding of the 2019 International Conference on Computer, Information and Telecommunication Systems*, 1–5. https://doi.org/10.1109/CITS.2019.8862127.

Hang, L., Choi, E., & Kim, D.-H. (2019). A novel EMR integrity management based on a medical blockchain platform in hospital. *Electronics (Switzerland)*, *8*(4). https://doi.org/10.3390/electronics8040467.

Hasavari, S., & Song, Y. T. (2019). A secure and scalable data source for emergency medical care using blockchain technology. In N. N. P. Song Y.-T. Acharya S. (Ed.), *Proceedings - 2019 IEEE/ACIS 17th International Conference on Software Engineering Research, Management and Application, SERA 2019* (pp. 71–75). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SERA.2019.8886792.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). International Journal of Medical Informatics Blockchain in healthcare and health sciences — A scoping review. *International Journal of Medical Informatics*, *134*(December 2019), 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040.

Hsu, C. L., Chen, W. X., & Le, T. V. (2020). An autonomous log storage management protocol with blockchain mechanism and access control for the internet of things. *Sensors (Switzerland)*, *20*(22), 1–32. https://doi.org/10.3390/s20226471.

Hu, S., Cai, C., Wang, Q., Wang, C., Luo, X., & Ren, K. (2018). Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization. *Proceedings - IEEE INFOCOM*, *2018-April*, 792–800. https://doi.org/10.1109/INFOCOM.2018.8485890.

Hur, J., Koo, D., Hwang, S. O., & Kang, K. (2013). Removing escrow from ciphertext policy attribute-based encryption. *Computers and Mathematics with Applications*, *65*(9), 1310–1317. https://doi.org/10.1016/j.camwa.2012.02.005.

Hur, J., & Noh, D. K. (2011). Attribute-based access control with efficient revocation in data outsourcing systems. *IEEE Transactions on Parallel and Distributed Systems*, *22*(7), 1214–1221. https://doi.org/10.1109/TPDS.2010.203.

Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (healthChain): Evaluation and proof-of-concept study. *Journal of Medical Internet Research*, *21*(8), 1–28. https://doi.org/10.2196/13592.

Iqbal, J., Umar, A. I., Amin, N., & Waheed, A. (2019). Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain. *International Journal of Distributed Sensor Networks*, *15*(9). https://doi.org/10.1177/1550147719875654.

Jamil, F., Ahmad, S., Iqbal, N., & Kim, D. H. (2020). Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors (Switzerland)*, *20*(8). https://doi.org/10.3390/s20082195.

Ji, Y., Zhang, J., Ma, J., Yang, C., & Yao, X. (2018). BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*, *42*(8), 147.

https://doi.org/10.1007/s10916-018-0998-2.

Jiang, P., Guo, F., Liang, K., Lai, J., & Wen, Q. (2017). Searchain : Blockchain-based private keyword search in decentralized storage. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.036.

Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A Review of Secure and Privacy-Preserving Medical Data Sharing. *IEEE ACCESS*, *7*, 61656–61669. https://doi.org/10.1109/ACCESS.2019.2916503.

Jivane, A. B. (2018). Time efficient privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*, *25*(1), 497–503. https://doi.org/10.1109/ICPCSI.2017.8392345.

Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., & Thompson, C. (2017). A Distributed-Ledger Consortium Model for Collaborative Innovation. *Computer*, *50*(9), 29–37. https://doi.org/10.1109/MC.2017.3571057.

Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. *Electronics (Switzerland)*, *9*(1). https://doi.org/10.3390/electronics9010094.

Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors (Switzerland)*, *20*(10), 1–21. https://doi.org/10.3390/s20102913.

Lee, H. A., Kung, H. H., Udayasankaran, J. G., Kijsanayotin, B. M. M. P., Marcelo, A. B., Chao, L. R., & Hsu, C. Y. (2020). An architecture and management platform for blockchain-based personal health record exchange: Development and usability study. *Journal of Medical Internet Research*, *22*(6), 1–15. https://doi.org/10.2196/16748.

Lee, T. F., Li, H. Z., & Hsieh, Y. P. (2020). A blockchain-based medical data preservation scheme for telecare medical information systems. *International Journal of Information Security*. https://doi.org/10.1007/s10207-020-00521-8.

Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6110 LNCS*(subaward 641), 62–91. https://doi.org/10.1007/978-3-642-13190-5_4.

Li, A., Wei, X., & He, Z. (2020). Robust Proof of Stake : A New Consensus Protocol for Sustainable Blockchain Systems, 1–15.

Li, Hongwei, Liu, D., Jia, K., & Lin, X. (2015). Achieving authorized and ranked multi-keyword search over encrypted cloud data. *IEEE International Conference on Communications*, *2015-Septe*, 7450–7455. https://doi.org/10.1109/ICC.2015.7249517.

Li, Hui, Fan, K., Yang, Y., Ren, Y., Wang, S., Ren, Y., … Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *JOURNAL OF MEDICAL SYSTEMS*, *42*(8), 1–11. https://doi.org/10.1007/s10916-018-0993-7.

Li, Huige, Tian, H., Zhang, F., & He, J. (2019). Blockchain-based searchable symmetric encryption scheme. *Computers and Electrical Engineering*, *73*, 32–45. https://doi.org/10.1016/j.compeleceng.2018.10.015.

Li, Huige, Zhang, F., He, J., & Tian, H. (2017). A Searchable Symmetric Encryption Scheme using BlockChain. Retrieved from http://arxiv.org/abs/1711.01030.

Li, J., Shi, Y., & Zhang, Y. (2017). Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage. *International Journal of Communication Systems*, *30*(1), e2942. https://doi.org/10.1002/dac.2942.

Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, *50 LNICST*, 89–106. https://doi.org/10.1007/978-3-642-16161-2_6.

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, *24*(1), 131–143. https://doi.org/10.1109/TPDS.2012.97.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, (Xiaoqi Li), 1–25. https://doi.org/10.1016/j.future.2017.08.020.

Lin, G., Hong, H., & Sun, Z. (2017). A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing. *IEEE Access*, *5*, 9464–9475. https://doi.org/10.1109/ACCESS.2017.2707126.

Liu, C., Zhu, L., & Chen, J. (2017). Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud. *Journal of Network and Computer Applications*, *86*, 3–14. https://doi.org/10.1016/j.jnca.2016.09.010.

Liu, H., Crespo, R. G., & Martínez, O. S. (2020). Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. *Healthcare*, *8*(3), 243. https://doi.org/10.3390/healthcare8030243.

Liu, S., Yu, J., Xiao, Y., Wan, Z., Wang, S., & Yan, B. (2020). BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT. *IEEE Internet of Things Journal*, *7*(9), 7851–7867. https://doi.org/10.1109/JIOT.2020.2993231.

Liu, X., Wang, Z., Jin, C., Li, F., & Li, G. (2019). A Blockchain-Based Medical Data Sharing and Protection Scheme. *IEEE ACCESS*, *7*, 118943–118953. https://doi.org/10.1109/ACCESS.2019.2937685.

Lu, Y. (2018). Blockchain: A Survey on Functions, Applications and Open Issues. *Journal of Industrial Integration and Management*, *03*(04), 1850015. https://doi.org/10.1142/S242486221850015X.

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*, *15*(January), 80–90. https://doi.org/10.1016/j.jii.2019.04.002.

Lv, Z., Hong, C., Zhang, M., & Feng, D. (2014). Expressive and secure searchable encryption in the public key setting. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8783*, 364–376. https://doi.org/10.1007/978-3-319-13257-0_21.

Mamta, & Gupta, B. B. (2019). An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud. *Concurrency Computation* , (March), 1–17. https://doi.org/10.1002/cpe.5291.

Mannaro, K., Baralla, G., Pinna, A., & Ibba, S. (2018). A blockchain approach applied to a teledermatology platform in the Sardinian Region (Italy). *Information (Switzerland)*, *9*(2). https://doi.org/10.3390/info9020044.

Margheri, A., Masi, M., Miladi, A., Sassone, V., & Rosenzweig, J. (2020). Decentralised provenance for healthcare data. *International Journal of Medical Informatics*, *141*, 104197. https://doi.org/10.1016/j.ijmedinf.2020.104197.

Meng, W., Li, W., & Zhu, L. (2019). Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2019.2921736.

Miao, Y., Deng, R., Liu, X., Choo, K. K. R., Wu, H., & Li, H. (2019). Multi-authority Attribute-Based Keyword Search over Encrypted Cloud Data. *IEEE Transactions on Dependable and Secure Computing*, 1–14. https://doi.org/10.1109/TDSC.2019.2935044.

Miao, Y., Liu, X., Choo, K. K. R., Deng, R. H., Li, J., Li, H., & Ma, J. (2019). Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting. *IEEE Transactions on Dependable and Secure Computing*, 1–15. https://doi.org/10.1109/TDSC.2019.2897675.

Miao, Y., Ma, J., Liu, X., Li, X., Jiang, Q., & Zhang, J. (2017). Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing. *IEEE Transactions on Services Computing*, *13*(6), 985–998. https://doi.org/10.1109/TSC.2017.2757467.

Miao, Y., Ma, J., Liu, X., Wei, F., Liu, Z., & Wang, X. A. (2016). m2-ABKS: Attribute-Based Multi-Keyword Search over Encrypted Personal Health Records in Multi-Owner Setting. *Journal of Medical Systems*, *40*(11), 1–12. https://doi.org/http://dx.doi.org/10.1007/s10916-016-0617-z.

Michalas, A. (2019). The Lord of the shares: Combining attribute-based encryption and searchable encryption for flexible data sharing. *Proceedings of the ACM*

Symposium on Applied Computing, *Part F1477*(April), 146–155. https://doi.org/10.1145/3297280.3297297.

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. I. (2019). Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. *Computer Standards and Interfaces*, *66*(March), 103343. https://doi.org/10.1016/j.csi.2019.04.002.

Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., & Balusamy, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing and Applications*, *32*(3), 639–647. https://doi.org/10.1007/s00521-018-3915-1.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, 9. https://doi.org/10.1007/s10838-008-9062-0.

Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. *Sustainability*, *11*(24), 7054. https://doi.org/10.3390/su11247054.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE ACCESS*, *7*, 66792–66806. https://doi.org/10.1109/ACCESS.2019.2917555.

Niu, S., Chen, L., Wang, J., & Yu, F. (2020). Electronic Health Record Sharing Scheme with Searchable Attribute-Based Encryption on Blockchain. *IEEE Access*, *8*, 7195–7204. https://doi.org/10.1109/ACCESS.2019.2959044.

Omar, A. Al, Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., Rahman, M. S., Al Omar, A., … Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, *95*, 511–521. https://doi.org/10.1016/j.future.2018.12.044.

P, P. K., P, S. K., & P.J.A., A. (2018). Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. *Journal of Network and Computer Applications*, *108*(December 2017), 37–52. https://doi.org/10.1016/j.jnca.2018.02.009.

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). *Blockchain and iot integration: A systematic survey*. *Sensors (Switzerland)* (Vol. 18). https://doi.org/10.3390/s18082575.

Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale : Challenges and reme dies base d on blockchain technology. *Health Policy and Technology*, *9*(1), 69–78. https://doi.org/10.1016/j.hlpt.2020.01.004.

Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry? *Journal of Industrial Information Integration*, *17*(August 2019), 100125.

https://doi.org/10.1016/j.jii.2020.100125.

Pham, H. L., Tran, T. H., & Nakashima, Y. (2018). A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract. In *2018 IEEE Globecom Workshops (GC Wkshps)* (pp. 1–6). IEEE. https://doi.org/10.1109/GLOCOMW.2018.8644164.

Pirretti, M., Traynor, P., Mcdaniel, P., & Waters, B. (2010). Secure Attribute-Based Systems. *Journal of Computer Security*, *18*(5), 799–837.

Pournaghi, S. M., Bayat, M., & Farjami, Y. (2020). MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. *Journal of Ambient Intelligence and Humanized Computing*, (0123456789). https://doi.org/10.1007/s12652-020-01710-y.

Prince, P. B., & Lovesum, S. P. J. (2020). Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System. *SN Computer Science*, *1*(5), 1–8. https://doi.org/10.1007/s42979-020-00246-4.

Qin, X., Huang, Y., Yang, Z., & Li, X. (2020a). A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *Journal of Systems Architecture*, (March), 101854. https://doi.org/10.1016/j.sysarc.2020.101854.

Qin, X., Huang, Y., Yang, Z., & Li, X. (2020b). LBAC: A Lightweight Blockchain-based Access Control Scheme for the Internet of Things. *Information Sciences*. https://doi.org/10.1016/j.ins.2020.12.035.

Radanović, I., & Likić, R. (2018). Opportunities for Use of Blockchain Technology in Medicine. *Applied Health Economics and Health Policy*. https://doi.org/10.1007/s40258-018-0412-8.

Rahman, M. A., Rashid, M., Barnes, S., Hossain, M. S., Hassanain, E., & Guizani, M. (2019). An IoT and Blockchain-Based Multi-Sensory In-Home Quality of Life Framework for Cancer Patients. In *2019 15TH INTERNATIONAL WIRELESS COMMUNICATIONS & MOBILE COMPUTING CONFERENCE (IWCMC)* (pp. 2116–2121). 345 E 47TH ST, NEW YORK, NY 10017 USA: IEEE.

Rajput, A. R., Li, Q., Ahvanooey, M. T., & Masood, I. (2019). EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain. *IEEE ACCESS*, *7*, 84304–84317. https://doi.org/10.1109/ACCESS.2019.2917976.

Ren, Y., Leng, Y., Zhu, F., Wang, J., & Kim, H.-J. (2019). Data storage mechanism based on blockchain with privacy protection in wireless body area network. *Sensors (Switzerland)*, *19*(10). https://doi.org/10.3390/s19102395.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046.

Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal*, *44*(3), 23–38. https://doi.org/10.12826/18333575.2015.0001.

Rhee, H. S., Park, J. H., Susilo, W., & Lee, D. H. (2009). Improved searchable public key encryption with designated tester. *Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security, ASIACCS'09*, (January), 376–379. https://doi.org/10.1145/1533057.1533108.

Rouhani, S. (2019). MediChain TM : A Secure Decentralized Medical Data Asset Management System. *ArXiv Preprint ArXiv:1901.10645*, (Section II), 1533–1538. https://doi.org/10.1109/Cybermatics.

Saravanan, M., Shubha, R., Marks, A. M., & Iyer, V. (2017). SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (Vol. 101, pp. 1–6). IEEE. https://doi.org/10.1109/ANTS.2017.8384099.

Sargent, R. G. (2013). Verification and validation of simulation models. *Journal of Simulation*, *7*(1), 12–24. https://doi.org/10.1057/jos.2012.20.

Schwartz, M., Gupta, S. K., Anand, D. K., & Kavetsky, R. (2012). Electronic Health Records: Privacy, Confidentiality, and Security. *AMA Journal of Ethics*, *14*(9), 712–719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209.

Services, I., Xu, L. Da, & Viriyasitavat, W. (2019). Application of Blockchain in Collaborative, 1–11. https://doi.org/10.1109/TCSS.2019.2913165.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access*, *7*, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373.

Shamshad, S., Minahil, Mahmood, K., Kumari, S., & Chen, C. M. (2020). A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications*, *55*, 102590. https://doi.org/10.1016/j.jisa.2020.102590.

Sharma, A., Sarishma, Tomar, R., Chilamkurti, N., & Kim, B. G. (2020). Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics (Switzerland)*, *9*(10), 1–14. https://doi.org/10.3390/electronics9101609.

Sharma, P., Jindal, R., & Borah, M. D. (2020). Blockchain Technology for Cloud Storage. *ACM Computing Surveys*, *53*(4), 1–32. https://doi.org/10.1145/3403954.

Song, D. X., Wagner, D., & Perrig, A. (2000). Practical techniques for searches on encrypted data. *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 44–55. https://doi.org/10.1109/secpri.2000.848445.

Steichen, M., Fiz, B., Norvill, R., Shbair, W., & State, R. (2018). Blockchain-Based, Decentralized Access Control for IPFS. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1499–1506). IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00253.

Sultan, N. H., Barbhuiya, F. A., & Sarma, N. (2017). A Universal Cloud User Revocation Scheme With Key-Escrow Resistance for Ciphertext-Policy Attribute-Based Access Control. *ACM International Conference Proceeding Series*, 11–18. https://doi.org/10.1145/3136825.3136877.

Sultan, N. H., Kaaniche, N., Laurent, M., & Barbhuiya, F. A. (2019). Authorized Keyword Search over Outsourced Encrypted Data in Cloud Environment. *IEEE Transactions on Cloud Computing*, *PP*(c), 1. https://doi.org/10.1109/TCC.2019.2931896.

Sun, J., Ren, L., Wang, S., & Yao, X. (2019). Multi-Keyword Searchable and Data Verifiable Attribute-Based Encryption Scheme for Cloud Storage. *IEEE Access*, *7*, 66655–66667. https://doi.org/10.1109/ACCESS.2019.2917772.

Sun, J., Yao, X., Wang, S., & Wu, Y. (2020). Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. *IEEE Access*, *8*, 59389–59401. https://doi.org/10.1109/ACCESS.2020.2982964.

Sun, W., Wang, B., Cao, N., Li, M., Lou, W., Hou, Y. T., & Li, H. (2014). Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. *IEEE Transactions on Parallel and Distributed Systems*, *25*(11), 3025–3035. https://doi.org/10.1109/TPDS.2013.282.

Sun, W., Yu, S., Lou, W., Hou, Y. T., & Li, H. (2016). Protecting Your Right: Verifiable Attribute-Based Keyword Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud. *IEEE Transactions on Parallel and Distributed Systems*, *27*(4), 1187–1198. https://doi.org/10.1109/TPDS.2014.2355202.

Sun, Y., Zhang, R., Wang, X., Gao, K., & Liu, L. (2018). A Decentralizing Attribute-Based Signature for Healthcare Blockchain. *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 1–9. https://doi.org/10.1109/ICCCN.2018.8487349.

Tang, F., Ma, S., Xiang, Y., & Lin, C. (2019). An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records. *IEEE Access*, *7*, 41678–41689. https://doi.org/10.1109/ACCESS.2019.2904300.

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*. https://doi.org/10.1016/j.jisa.2019.102407.

Thwin, T T, & Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. *Security and*

Communication Networks, 2019. https://doi.org/10.1155/2019/8315614.

Thwin, Thein Than, & Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. *SECURITY AND COMMUNICATION NETWORKS*. https://doi.org/10.1155/2019/8315614.

Uddin, M A, Stranieri, A., Gondal, I., & Balasubramanian, V. (2019). A Decentralized Patient Agent Controlled Blockchain for Remote Patient Monitoring. In *International Conference on Wireless and Mobile Computing, Networking and Communications* (Vol. 2019-Octob, pp. 207–214). IEEE Computer Society. https://doi.org/10.1109/WiMOB.2019.8923209.

Uddin, Md Ashraf, Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. *IEEE Access*, *6*, 32700–32726. https://doi.org/10.1109/ACCESS.2018.2846779.

Viriyasitavat, W, Anuphaptrirong, T., & Hoonsopon, D. (2019). When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. *Journal of Industrial Information Integration*, *15*, 21–28. https://doi.org/10.1016/j.jii.2019.05.002.

Viriyasitavat, Wattana, Bi, Z., & Hoonsopon, D. (2019). Blockchain Technology for Applications in Internet of Things — Mapping From System Design Perspective, *6*(5), 8155–8168.

Viriyasitavat, Wattana, & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*(June 2018), 32–39. https://doi.org/10.1016/j.jii.2018.07.004.

Viriyasitavat, Wattana, Xu, L. Da, Bi, Z., & Pungpapong, V. (2019). Blockchain and Internet of Things for Modern Business Process in Digital Economy—the State of the Art. *IEEE Transactions on Computational Social Systems*, *6*(6), 1420–1432. https://doi.org/10.1109/TCSS.2019.2919325.

Viryasitavat, W., Da Xu, L., Bi, Z., & Sapsomboon, A. (2018). Blockchain-based business process management (BPM) framework for service composition in industry 4.0. *Journal of Intelligent Manufacturing*. https://doi.org/10.1007/s10845-018-1422-y.

Wang, H., & Song, Y. (2018). Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. *Journal of Medical Systems*, *42*(8), 152. https://doi.org/10.1007/s10916-018-0994-6.

Wang, J., Han, K., Alexandridis, A., Chen, Z., Zilic, Z., Pang, Y., … Piccialli, F. (2019). A blockchain-based eHealthcare system interoperating with WBANs. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2019.09.049.

Wang, S., Gao, T., & Zhang, Y. (2018). Searchable and revocable multi-data owner attribute-based encryption scheme with hidden policy in cloud storage. *PLoS ONE*, *13*(11), 1–19. https://doi.org/10.1371/journal.pone.0206126.

Wang, S., Wang, X., & Zhang, Y. (2019). A Secure Cloud Storage Framework With Access Control Based on Blockchain. *IEEE Access*, *7*, 112713–112725. https://doi.org/10.1109/access.2019.2929205.

Wang, S., Yao, L., Chen, J., & Zhang, Y. (2019). KS-ABESwET: A Keyword Searchable Attribute-Based Encryption Scheme with Equality Test in the Internet of Things. *IEEE Access*, *7*, 80675–80696. https://doi.org/10.1109/ACCESS.2019.2922646.

Wang, S., Yao, L., & Zhang, Y. (2018). *Attribute-based encryption scheme with multi-keyword search and supporting attribute revocation in cloud storage*. *PLoS ONE* (Vol. 13). https://doi.org/10.1371/journal.pone.0205675.

Wang, S., Ye, J., & Zhang, Y. (2018). A keyword searchable attribute-based encryption scheme with attribute update for cloud storage. *PLoS ONE*, *13*(5), 1–19. https://doi.org/10.1371/journal.pone.0197318.

Wang, S., Zhang, D., & Zhang, Y. (2019). Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable. *IEEE ACCESS*, *7*, 102887–102901. https://doi.org/10.1109/ACCESS.2019.2931531.

Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, *6*, 38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611.

Wang, W., & Hoang, D. T. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*, *7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108.

Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain. *IEEE Access*, *7*, 136704–136719. https://doi.org/10.1109/ACCESS.2019.2943153.

Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q., & Zheng, D. (2019). Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Annals of Telecommunications Volume*, (74), 401–411. https://doi.org/https://doi.org/10.1007/s12243-018-00699-y Efficient.

Wu, A., Zheng, D., Zhang, Y., & Yang, M. (2018). Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing. *Sensors (Switzerland)*, *18*(7), 1–17. https://doi.org/10.3390/s18072158.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE ACCESS*, *5*, 14757–14767. https://doi.org/10.1109/ACCESS.2017.2730843.

Xu, Li Da, Xu, E. L., & Li, L. (2018). Industry 4 . 0 : state of the art and future trends, *7543*. https://doi.org/10.1080/00207543.2018.1444806.

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. *IEEE*

INTERNET OF THINGS JOURNAL, *6*(5, SI), 8770–8781. https://doi.org/10.1109/JIOT.2019.2923525.

Xu, Lei, Xu, C., Liu, J. K., Zuo, C., & Zhang, P. (2020). Building a dynamic searchable encrypted medical database for multi-client. *Information Sciences*, *527*, 394–405. https://doi.org/10.1016/j.ins.2019.05.056.

Yang, X., Li, T., Pei, X., Wen, L., & Wang, C. (2020). Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology. *IEEE Access*, *8*, 45468–45476. https://doi.org/10.1109/ACCESS.2020.2976894.

Yazdinejad, A., Srivastava, G., Parizi, R. M., Dehghantanha, A., Choo, K.-K. R., & Aledhari, M. (2020). Decentralized Authentication of Distributed Patients in Hospital Networks using Blockchain. *IEEE Journal of Biomedical and Health Informatics*, *2194*(c), 1–1. https://doi.org/10.1109/jbhi.2020.2969648.

Yin, H., Xiong, Y., Zhang, J., Ou, L., Liao, S., & Qin, Z. (2019). A key-policy searchable attribute-based encryption scheme for efficient keyword search and fine-grained access control over encrypted data. *Electronics (Switzerland)*, *8*(3), 1–20. https://doi.org/10.3390/electronics8030265.

Yin, H., Zhang, J., Xiong, Y., Ou, L., Li, F., Liao, S., & Li, K. (2019). CP-ABSE: A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme. *IEEE Access*, *7*, 5682–5694. https://doi.org/10.1109/ACCESS.2018.2889754.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. *PLoS ONE*, *11*(10), 1–27. https://doi.org/10.1371/journal.pone.0163477.

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Attribute based data sharing with attribute revocation. *Proceedings of the 5th International Symposium on Information, Computer and Communications Security, ASIACCS 2010*, 261–270. https://doi.org/10.1145/1755688.1755720.

Zhang, B., & Zhang, F. (2011). An efficient public key encryption with conjunctive-subset keywords search. *Journal of Network and Computer Applications*, *34*(1), 262–267. https://doi.org/10.1016/j.jnca.2010.07.007.

Zhang, J., Xue, N., & Huang, X. (2016). A Secure System for Pervasive Social Network-Based Healthcare. *IEEE Access*, *4*, 9239–9250. https://doi.org/10.1109/ACCESS.2016.2645904.

Zhang, L., Hu, G., Mu, Y., & Rezaeibagha, F. (2019). Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system. *IEEE Access*, *7*, 33202–33213. https://doi.org/10.1109/ACCESS.2019.2902040.

Zhang, L., Su, J., & Mu, Y. (2020). Outsourcing Attributed-Based Ranked Searchable Encryption with Revocation for Cloud Storage. *IEEE Access*, *8*, 104344–104356. https://doi.org/10.1109/ACCESS.2020.3000049.

Zhang, P., Schmidt, D. C., White, J., & Dubey, A. (2019). Consensus mechanisms and information security technologies. *Advances in Computers*, *115*, 181–209. https://doi.org/10.1016/bs.adcom.2019.05.001.

Zhang, R., Xue, R., & Liu, L. (2018). Searchable encryption for healthcare clouds: A survey. *IEEE Transactions on Services Computing*, *11*(6), 978–996. https://doi.org/10.1109/TSC.2017.2762296.

Zhang, R., Xue, R., Yu, T., & Liu, L. (2016). Dynamic and efficient private keyword search over inverted index-based encrypted data. *ACM Transactions on Internet Technology*, *16*(3), 1–20. https://doi.org/10.1145/2940328.

Zhang, Yinghui, Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based Encryption for Cloud Computing Access Control: A Survey. *ACM Computing Surveys*, *53*(4). https://doi.org/10.1145/3398036.

Zhang, Yongbin, Cui, M., Zheng, L., Zhang, R., Meng, L., Gao, D., & Zhang, Y. (2019). Research on electronic medical record access control based on blockchain. *International Journal of Distributed Sensor Networks*, *15*(11). https://doi.org/10.1177/1550147719889330.

Zheng, H., Shao, J., & Wei, G. (2020). Attribute-based encryption with outsourced decryption in blockchain. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-020-00918-1 Attribute-based.

Zheng, Q., Xu, S., & Ateniese, G. (2014). VABKS: Verifiable attribute-based keyword search over outsourced encrypted data. In *Proceedings - IEEE INFOCOM* (pp. 522–530). https://doi.org/10.1109/INFOCOM.2014.6847976.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2016). Blockchain Challenges and Opportunities : A Survey. *International Journal of Web and Grid Services*, (October), 1–24. https://doi.org/10125/41338.

Zhou, Y., Li, N., Tian, Y., An, D., & Wang, L. (2020). Public key encryption with keyword search in cloud: A survey. *Entropy*, *22*(4), 1–24. https://doi.org/10.3390/E22040421.