International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 7 ǁ July 2023 ǁ PP. 249-262

Role of Block Chain in Ensuring Network Security of EHR

Vidson Vishal Dsouza *Department of Tech & Software University of Europe for AppliedScience Potsdam, Germany sanjeev.patil@ue-germany.de*

Prof. Dr Mohammed Nazeh Alimam *Department of Tech & Software University of Europe for Applied Science Potsdam, Germany mohammednazeh.alimam@ue-germany.de*

Prof. Dr Rand Kouatly *Department of Tech & Software University of Europe for AppliedScience Potsdam, Germany rand.kouatly@ue-germany.de*

Abstract—*The thesis paper aims at evaluating the overall efficacy of block chain management in network security or cyber security of EHR (electronic health record system). In this context, the notions of blockchain and network security have been explained on an overall basis. Furthermore, the current challenges of cyber security have been addressed. The challenges include social engineering, ransom ware, distribution of DDos, cloud computing issues, enhanced use of artificial intelligence and crypto attacks. Apart from that, the implementation challenges of block chain have also been addressed under this proposal. The challenges include lack of "adoption", the ever-increasing cost of implementation, scalability, privacy challenges and security challenges, the problem of excessive energy consumption, the lower availability of skilled workforce required for the facilitation of block chain management, tough integration techniques with the European legal system and interoperability. The relevant study states that block chain solution implementation is regarded as the newest cyber security approach, which can facilitate the notion of network protection to a brand-new level. It should also be mentioned that the empirical data collection method of secondary data will be used for the purpose of conducting the relevant research work. To state concisely, the research will be based on 10 peer reviewed journals and articles and results and analysis will be based on the collective opinion on the basis of secondary data analysis.*

Keywords: *Blockchain, Cyber Security, EHR, Big Data, CloudComputing, Cyberattacks*

Date of Submission: 11-07-2023 Date of acceptance: 24-07-2023

I. INTRODUCTION

Due to the extensive usage of big data in a number of areas (science, engineering, business, etc.), security and privacy concerns related to big data are becoming an increasingly popular subject of research [1] Somewhere in the neighbourhood of a quintillion bytes of information is created every day in a wide variety of formats and domains, including but not limited to online communities, sensor networks, digital images/videos, mobile phones, GPS signals, logs of financial dealings, weblogs, medical files/archives, military records/surveillance, online markets, and in-depth scientific studies. The term "big data" is used to refer to this massive amount of data [2]

Electronic health data (EHD) or electronic health records have replaced paper records in the healthcare industry as a result of big data's growth (EHRs). EHD includes a patient's personal information as well as their medical history, prescriptions, allergies, vaccination status, laboratory test results, x-ray images, billing information, and more. The use of electronic health records (EHRs) has various advantages, including improved timeliness and accuracy of clinical data access, andmore streamlined clinical operations.

Improvements in clinical decision-making support, reduced medical mistakes, higher patient safety, reduced healthcare costs, and more efficient healthcare systems are all possible outcomes of this work. More than 90% of healthcare facilities in Australia and throughout the world have embraced EHD systems, realizing the advantages given by these systems for facilitating optimal medical resource allocation and efficient healthcare [3].

Electronic health records (EHRs) have also been extensively employed to facilitate the creation, storage, management, and on-demand access to healthcare information for both healthcare practitioners and patients. In most cases, cloud services provide the greatest infrastructure because of the reduced price of data storage, processing, and updating that they offer.

The healthcare sector is making substantial use of cloud computing, a rapidly developing paradigm in

digital technology [4]. Cloud networks are playing an increasingly important role in today's era of big data because of their ability to store and transfer endless quantities of data, making them ideal for the widespread dissemination of health information. It streamlines the process of creating, storing, and retrieving data in real time for healthcare providers, doctors, and patients. Data privacy and security issues arise due to the fact that it is kept on a decentralized network of distant servers that are managed as one ecosystem and accessed from many placesby numerous users.

Moreover, since most medical data is very delicate and must be kept secret, storing it on external servers inherently raises these vulnerabilities [5]. Security and privacy are undeniably the most difficult and worrying issues. Inadequate management of large data has been shown in several studies to compromise user privacy [6].

The following are some privacy and security issues that need to be addressed in the context of big data: The inference of new facts about a person when that person's personal information is joined with external huge data sets may disclose truths about that person that in addition to the data owner and any other third parties not wanting to know this, the person may not want anybody else to know this.

The use of big data in law enforcement will increase the likelihood that some tagged people may be subjected to adverse consequences, as is already visible in underdeveloped nations with a large digital divide. In light of this, and the ease with which hackers may obtain publicly accessible health information, there needs to be a safer, more streamlined, and more productive method for stakeholders to share and receiveinformation [7].

Confidential patient data stored in the cloud presents a significant challenge to effective data use and processing. Since much EHD is delicate and must be kept private, protecting medical records in storage is a top priority. The goal of this study is to provide a task-based framework for the safe and efficient transfer of patient information between variousentities without compromising patient privacy.

With the exception of life-or-death situations, the patient in a Patient-Controlled Electronic Health Record System (PCEHR) is the only person who may provide permission for the release of the patient's information to any third parties; blockchain is one way to eliminating most of the faults of the present scattered structure.

With so much private data stored in the cloud, outside of the user's immediate control, it's important to take extra precautions while storing data online, the healthcare business is more vulnerable to privacy breaches and unauthorized record access, Institutions in the healthcare industry.

The primary concern is the freedom of a person to conduct their daily lives without fear of observation or intervention from others, whether private entities or the state. Data collected from them must be securely stored and appropriatelyhandled, and patients' rights to privacy must be protected.

Due to the importance of protecting sensitive health information, this study reviews the existing taxonomy of cloud based EHR privacy preservation techniques and analyses many blockchain technologies to determine how best to integrate their features into the current security architecture. One of the goals of this study is to benefit the patients and thecommunity. Problems of the following kind have been discovered during study.

RQ1: The need for a solution to the current limitations of e- health data storage systems and asks how blockchain technology may be used to provide an effective access controlmechanism and encryption approach.

RQ2: What are the steps involved in designing, developing, and analyzing a new framework to prove patient privacy anddata security?

RQ3: What are the challenges that need to overcome for the best results for EHR system for security system?

RQ4: How is it possible for Blockchain to keep the "ever- growing" number of patient medical records indefinitely?

Purpose of our research is to determine which electronic health records (EHR) have been designed with safety in mind and to investigate and assess the good influence that blockchain technology has had on the growth of cyber security for HER. Discover available techniques of the block chain solutions that may assist in security management but do not need any requirements linked to crypto currency. Conduct research and evaluation on the potential applications of blockchain technology in EHR network security.

II. LITERATURE REVIEW

After an exhaustive literature review, we have settled on the following goals for this chapter. Some pressing concerns and promising avenues for further study of the safety and privacy of electronic health data are addressed in this essay (EHRs). These include but are not limited to: 1) the security and privacy of electronic health records; 2) the security and privacy requirements of electronic health data stored in the cloud; 3) the architecture of cloud-based EHRs; and 4) the various cryptographic and non-cryptographic approaches to EHRs. Cryptographic techniques such as Symmetric Key Encryption (SKE), Public Key Encryption (PKE), Attribute - Based Encryption (ABE), Searchable Symmetric Encryption (SSE), Proxy Re-encryption (PRE), and Homomorphic Encryption (HE) are all extensively discussed in Chapter 16 of Security and Privacy Requirements of e-Health Data in the Cloud. Techniques that don't use encryption, like Discretionary Hash

Function Pseudo-Role Attribute-based Access Control (PR-ABAC) is a multi-layer access control (MLAC) method that combines attributes and roles to guarantee the secure exchange of electronic health records (EHR) among a group of personnel working together. In this review, the benefits and drawbacks of existing privacy-preserving methods as well as the research problems associated with them are investigated. Following this, a new model that is supported by blockchain technology is proposed. This model can address some of these limitations while also providing a secure and efficient means of protecting electronichealth records.

2.1 Definition of research questions Need for Data Isolation and Encryption in Cloud Healthcare Systems

In this era of big data, outsourcing medical records to cloud servers poses a variety of potential vulnerabilities to cyber- attacks [8]. These vulnerabilities include, but are not limited to, information leaks, denial of service attacks (DoS), man- in-the-middle attacks, and ransom ware assaults. Therefore, the protection and security of patient data is an imperative need in order to maintain patient confidentiality. The following are some of the most important criteria for privacy and security that must be met by e-health systems: One of them is data integrity, which ensures that the medical records of patients have not been altered in any manner. Second, maintaining the confidentiality of patient information is very necessary to prevent potentially damaging information from falling into the wrong hands. When it comes to the protection of sensitive information, encryption is the most effective solution currently available. Protects patients' private health information by limiting access to just those organizations who are authorized to see it (point number three in Overview of E-health Systems Hosted in the Cloud, point number seventeen overall). 4) Accountability, also known as the need, to provide reasons for one's actions and to defend one's decisions, is a fundamental principle that is upheld by individuals as well as by institutions. Five) It is vital to conduct audits to keep track of user activity, as well as to reassure users that the confidentiality of their health information will be maintained. Non-repudiation is the sixth principle, and it states that neither the sender nor the receiver may dispute that they are who they claim to be. This applies to both the sender and the recipient. Following the loss of medical data, patients, and doctors, for example, have few legal options available to them. 7) Anonymity ensures that the identity of the subject is concealed from the cloud servers that store the patient's medical information [9]. As a result of the centralized, mainframe computing model that is owned by the cloud provider and the fact that the model is less patient-centric, cloud computing environments pose a greater threat to patients' medical records. One of the most significant drawbacks of cloud storage is this. Even though cloud technologies follow tight security rules, they are not yet a foolproof answer for adoption in e-health because of security concerns. Several approaches to cloud protection are reviewed, and some recent improvements along with the benefits and drawbacks of using them.

Some of the more complicated privacy-preserving frameworks for e-health can be implemented, but the fact that others aren't chosen due to security concerns shows that these frameworks don't provide a foolproof answer for the e-healthindustry.

2.2 An Outline of Cloud-Based Healthcare Systems

The electronic health system is a relatively recent innovation in the field of medicine that centers on the utilization of digital channels for the purposes of organization and communication. A standardized compilation of a patient's electronic health record (EHR) or electronic medical record (EMR) is referred to as an electronic health record (EHR) or electronic medical record (EMR) [9]. These files contain a patient's name and address, as well as their medical history, prescriptions, test results, x-rays, billing details, and Social Security number. In addition, these files also contain the patient's x-rays.

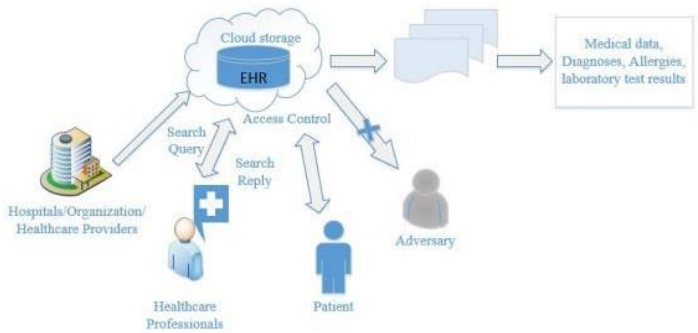

Figure 1: The Cloud Healthcare InformationSystems Design Framework

2.3 Cloud Computing Security: E-Current Health'sStatus and Future Research Opportunities

Electronic health data (EHDs) are all examples of digital records that have replaced paper-based records as the digitalization of information has progressed in the twenty- first century (EHD). Unlike electronic health records (EHRs) and medical records (EMRs), personal health records (PHRs) are maintained and checked on a regular basis by the patient or their loved ones. EHD, short for electronic health records or computerized patient records, is a standardized database including patients' up-to-date, highly detailed digital health histories (Yi et al, 2017). These files include a plethora of information on patients, including their medical histories, personal details, medications, immunization status, laboratory test results, and more. Electronic health record (EHR) systems offer several advantages over manual filing methods. Electronic health records (EHRs) save money in terms of fewer staff hours, less space required for storage, and less environmental impact [11]. Electronic health records (EHRs) provide several benefits, such as improved accessibility to clinical data, more efficient clinical processes, fewer medical mistakes; higher patient safety, lower healthcare costs, and more informed clinical decision- making. More than 90% of Australian healthcare facilities have implemented an EHD system to better allocate medical resources and provide more efficient treatment to patients [11]. Multiple users have confirmed and attested to EHD's capacity to improve healthcare administration. However, there are special difficulties associated with the transfer of medical records from traditional healthcare systems to e-healthcare.

The healthcare sector is making significant use of the cloud computing paradigm, a relatively new development in digital technology [12]. It not only makes it simple to keep track of medical records, but also to share them with other people. Amongst numerous parties involved. In this era of big data, when data volumes may grow exponentially, cloud networks are playing an increasingly important role in health care information dissemination [13].

It makes it easy for healthcare professionals, physicians, and patients to create, save, and retrieve healthcare information, regardless of time or location. The cloud's ability to store, retrieves, analyze, and update data efficiently and cheaply has huge implications for businesses. Data security and privacy are at risk since it is housed and processed by a dispersed and distributed set of distant servers that are managed as a single ecosystem and accessible from various places by many users. Additionally, most medical data is very private and sensitive, thus storing it on external server's compounds these risks [14]. Primary care doctors, therapists, specialists, and medical, dental, vision, and other insurance companies are only some of the many healthcare providers a patient may have [15]. Due to the open nature of health data in the public sphere, there must be a safer, more streamlined, and more productive means of information exchange amongst all parties involved.

Although electronic health records (EHRs) face several threats in the healthcare industry, the most significant concern is the confidentiality and security of patient information [14]. Malware assaults, which may jeopardize the privacy and security of patient information, and distributed denial-of-service (DDoS) attacks, which can cripple a system's capacity to treat patients quickly and effectively, are only two examples of the threats that exist. The effects of cyber-attacks, such as those brought on by ransom ware; extend well beyond the obvious monetary costs and privacy leaks [16]. More than a million American patients' social security numbers were among the personal health details acquired by hackers who hacked [16] into the database of a leading hospital group's community health systems (CHS). Distributed denial of service (DDoS) attacks on the websites of many hospitals were launched by the online vigilante group Anonymous in a similar incident [17] disrupting medical services. These instances demonstrated the need of safeguarding PHI in EHR by preserving its secrecy, reliability, accessibility, and privacy. The effect of unauthenticated access to health data on social, economic, political, and cultural issues highlights the importance of cyber security's role in preventing, detecting, and acting uponsuch access.

The Health Insurance Portability and Accountability Act (HIPAA) mandate that healthcare providers safeguard their patients' personal information [18]. Many strategies have been tried and tested to ensure the privacy of digital health records stored in the cloud.

Nevertheless, owing to safety considerations, not all the cutting-edge privacy-preserving methods that ensure the security of cloud data can be used to e-health. Cloud computing reliance on a centralized, mainframe computing architecture under the authority of the cloud provider makes patient medical records more susceptible. This is a major disadvantage of cloud computing. Although cloud methods use stringent security standards, they are not yet stable enough for broad usage in e-health. Fingerprints, irises, speech patterns, and facial templates, among others, are encrypted before being uploaded to the cloud [19]. Using this method, users may be certain that their private data is as safe as can be against collusion attacks. With the ability to encrypt data at rest and keep it in the cloud, e-health clouds might be utilized to effectively store data. Due to the sensitive nature of medical information and the fact that the data is only accessible by the owner of the database, this method is less acceptable.

The lack of patient focus and the computational impossibility of the approach mean that it cannot be considered as a viable option for electronic health records. To improve security and performance, researchers in

presented a hybrid ciphertext- policy attribute-based encryption (CP-ABE) access control technique for public cloud storage. [20] offer an auditing mechanism as a secure and efficient access control strategy to address the single-point performance bottleneck that plagues most current CP-ABE systems. These systems [21],

[20] are sophisticated access control schemes with strong security measures, but they cannot be immediately applied to e-health because they cannot ensure protection from insider assaults due to it being regulated by a central authority and various attribute authorities. As a way for cloud storage providers to produce user secrets with just the cipher text they had stored, Deniable ABE was proposed [22] which is an adaption of Waters' CP-ABE method. This method uses both ABE and symmetric key encryption to provide multi-privileged access control for PHRs by encrypting data from several patients with the same access policy at once [22]. Cloud computing services use this model's encrypted prediction models to make medical diagnoses without revealing any personally identifying information about the patient. Current studies investigate a variety of encryption methods to address cloud computing's security issues [24]. Two-factor authentication, in which the user's identity is verified at both the network and cloud gateways, was proposed [25]. This method limits denial-of-service assaults and boosts cloud computing's efficiency. An identity-based hierarchical paradigm, together with the accompanying encryption and signature, was presented for use in cloud computing by [20]. [26] suggested a cryptographic architecture for safe data management that makes use of ID- based cryptography by encrypting and transmitting data with clients in such a way that no malevolent user may see the datawithout the owner's permission.

However, the computational complexity and scalability concerns make these approaches inappropriate for use with health information, even though they impart a high degree of data privacy. On the other hand, other work has created a private, secure CP-ABE where the access policy is concealed and allowed access is controlled by constant-length keys [27]. Identity-based revocable storage encryption [27] demonstrated both forward and backward ciphertext security (IBE). The bulk of the existing secure cloud storage solutions lack support for dynamic user management, have a significant performance overhead, and have limited access control. This article offers a workaround by presenting an attribute-based, secure cloud storage system with a history of provenance. Granular, well-structured access to medical records is only possible with ABE schemes, but their high computational cost makes appropriate implementation on EHRs impractical [27]. Managing access control rules becomes more difficult as the number of attributes in the access hierarchy grows [28]. Despite its numerous advantages, cloud computing introduces new safety and regulation concerns to the healthcare sector. Patients' confidentiality may be jeopardized if their health records are stored on distant servers. Data security and data integrity facenew issues with cloud storage and retrieval [29].

Providers of cloud computing services also play an important part in areas such as transaction analysis, access control, data security, and service integration, which is a major drawback. There has been an increase in sophisticated cyber-attacks in recent years, which threatens the confidentiality and integrity of electronic health records. Therefore, it is crucial to ensure the security of e-health records in a public, private, or hybrid cloud setting. Therefore, this study proposes a blockchain- based electronic health records system that is permission andpatient-centric, thereby removing most of the currentbottlenecks in the cloud.

2.4 EHR Privacy Protections: A Taxonomy

In this part, we'll talk about the difficulties associated with using cryptographic and non-cryptographic ways in e-health, as well as review the many studies that have been conducted on these two methods. Multiple methods for keeping cloud- stored information safe, private, and anonymous are also examined. Furthermore, certain searchable encryption (SE) methods are described for accessing cloud-based encrypted data. Normal search methods cannot be used since the data is encrypted and stored on external cloud services. Although it is difficult to search encrypted data, a method called searchable symmetric encryption (SSE) has been described that makes it possible to do keyword searches on encrypted cloud data. Unlike other polls, our study takes a methodical approach to investigating the many means through which electronic health records may be kept secure in the cloud.

In addition, the survey details the state-of-the-art approaches to cloud computing security and the obstacles to their study, while also including the prospective advantages of the blockchain approach to make up for their deficiencies. Finally, we conclude by outlining the unanswered questions and potential new avenues for study in the field of data privacy and security. Comparatively, non-cryptographic systems use access control mechanisms like RBAC, ABAC, IBAC, etc., whereas cryptographic strategies utilize encryption techniques like symmetric key encryption, public key encryption, and numerous more cryptographic primitives. In this section, we provide taxonomy of the techniques used to protect individual privacy, as shown in Fig. 2.

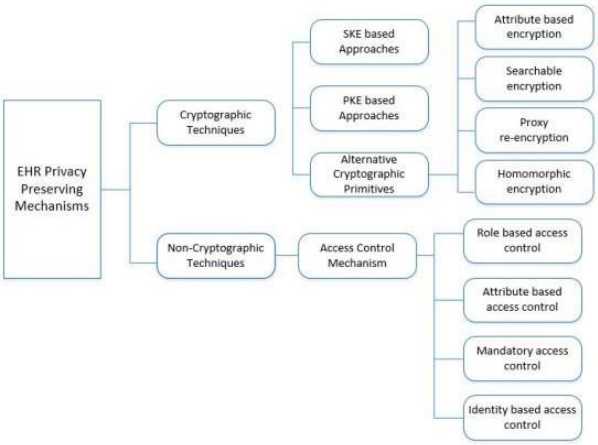

Figure 2: Grouping EHR Privacy ProtectionMethods

2.5 Cryptographic Approaches

Both symmetric (where both encryption and decryption use the same key) and asymmetric (where the keys are different) methods exist for protecting sensitive information (using distinct keys for each). This analysis considers the likes of public key encryption (PKE) and symmetric key encryption (SKE) in addition to other cryptographic basics. Data encryption and decryption in PKE systems requires a pair of public and private keys, but in SKE-based methods, just one secret key is needed. Attribute-based encryption (ABE), searchable encryption (SE), proxy re-encryption (PRE), homomorphism encryption (HE), identity-based encryption (IBE), etc. are all examples of cryptographic primitives, and there are many more. A policy-based authorization architecture that does not depend on cryptography might include a wide variety of access control technologies such as role-based access control (RBAC), attribute-based access control (ABAC), mandatory access control (MAC), and identity-based access control (IBAC). This section offers a thorough analysis of the research published on the topic of using SKE, PKE, and other cryptographic primitives to protect the privacy and integrity of e-health solutions.

2.6 Hypothesis

H1: Healthcare blockchain technology has a significanceimpact on Patient Identity
H2: Health blockchain technology has a significance impacton Data Security
H3: Healthcare Blockchain technology has a significanceimpact on Data monitoring.

2.7 Theoretical Framework

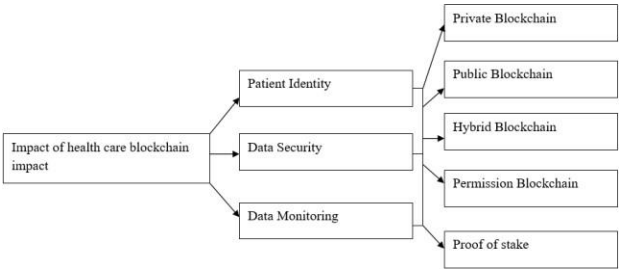

Figure 3: Theoretical Framework

III. METHODOLOGY

For the proposed problem we have choose to do qualitative analysis, systematic analysis and Meta analysis is done for data analysis and results. In this investigation, a mixed methodology was used, which included the collection of both quantitative and qualitative data. The conceptualization and evaluation of an architectural framework for a block chain- based healthcare record system is the primary objective of this research. To accomplish this goal, it is vital to first have an in-depth understanding of the problem that is posed by the existing health record system. For gaining a deeper comprehension of the flaws in the functioning of the present health care system, both qualitative and quantitative information was amassed via the use of questionnaires and surveys. During the whole process of evaluating the intended architecture, qualitative input was obtained and collected. An open-ended questionnaire was prepared and sent to medical professionals to ascertain the level of satisfaction those individuals had with the building's most notable features.

Proposed Method for this research is systematic review, Systematic reviews are in-depth analyses and

syntheses of relevant data, conducted according to a predetermined set of guidelines. Proficient meteorologists usually carry it out with the help of subject matter specialists. Formalizing research topics is the first stage in every systematic review.

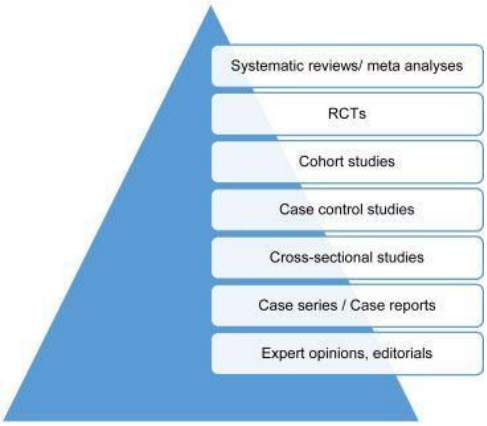

Figure 4 Systematic Literature Review Method

In this study, a deductive approach was taken to test the hypothesis that architecture of healthcare records based on block chain technology would be superior to the current system. To address the fundamental challenges that are currently confronting the healthcare industry all over the world, with a specific emphasis on developing countries, the purpose of this study was to design a health record system that is based on block chain technology. Before designing the architecture that is based on block chains, it was necessary to first collect the technical information that is associated with multiple block chains. To determine which block chain to use, in-depth research into the structure of the system and its primary characteristics was required. Interviews with industry professionals were carried out with the goal of gleaning the maximum amount of technical knowledge feasible on the block chain. The architecture was built with consideration given to the most significant gaps in the health business as well as numerous block chains and the applications of those block chains. This study's primary aim is to verify theoretical frameworks for building design. Future scalability, portability, efficiency, and security were all considered throughout the technical review of the design. The Architectural Trade-off Analysis Method was employed for this technical validation (ATAM). Validating the architecture for qualities like modifiability, portability, extensibility, and in-error-ability, ATAM is a scenario-based architectural assessment method. This method may be broken down into

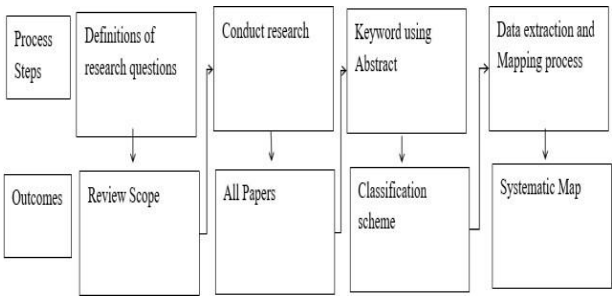

Figure 5. The systematic Mapping Process Step

its four primary components: the introduction, the research and analysis, the testing, and the final report. The replies of healthcare practitioners to a questionnaire demonstrated their contentment with the way the design performed its functions. The participants were given a comprehensive walk through of the architecture's process and then asked to score how successful it was in relation to a variety of different criteria, such as interoperability, data security and privacy, medical research, and so on.

3.1 Definition of research questions

RQ1: The need for a solution to the current limitations of ehealth data storage systems and asks how block chain technology may be used to provide an effective access control mechanism and encryption approach.

Block chain technology is used to address the problems with EHR systems. Block chain technology, in its simplest form, is a distributed digital ledger that may be used to record and verify transactions. There is no way to alter, manipulate, or hide this data. Patienter is a system for managing and analyzing data related to a

population's health. It provides doctors and hospitals with information that may improve treatment. Incorporating block chain technology, which gathers healthcare data from companies across silos, may help achieve this goal.

RQ2: What are the steps involved in designing, developing, and analyzing a new framework to prove patient privacy and data security?

Multi-specialty hospitals and solo offices alike are making use of the same improvements in healthcare technology that have allowed for the former to provide better treatment for their patients. Perhaps you saw the doctor making notes on their computer, iPad, or smartphone during your appointment. You probably predicted correctly that they aren't merely making fresh paper records but rather using EHR software (EHR). The use of electronic health records (EHRs) has various benefits, including better patient care and higher physician efficiency. There is an increase in both security and privacy issues related to electronic health records, even though EHR make it easier for clinics to keep track of patient medical details.

RQ3: What are the challenges that need to overcome for the best results for EHR system for security system?

Privacy concerns, incompatibility with existing systems, and disruptions to existing workflows are among the most significant obstacles to implementing an EHR system. The program is expensive, and its deployment will need a cash outlay.

Electronic Health Record integration may make a major impact for a healthcare facility. The healthcare industry, there is a lot of room for improvement in the use of machine learning to practice management and electronic health record (EHR) systems. To help you with the EHR integration process, the Intellect soft team has compiled our best practices and client experience to provide you with insights into not only the benefits, but also the key problems, and solutions. Your firm will flourish indefinitely if you take the initial step toward becoming more digital and patient focused. A technology like electronic health records (EHR) could completely revolutionize and automate your healthcare organization.

RQ4: How is it possible for Block chain to keep the "ever- growing" number of patient medical records indefinitely? Block chain technology has several potential medical applications. Securely sharing patient medical information, overseeing the distribution of pharmaceuticals, and assisting in the decoding of genetic code are all made possible by distributed ledger technology.

It offers a possible answer to issues plaguing the existing state of health IT. Block chain's benefits lie in its capacity to provide compatibility across different systems, as well as in the reliability, safety, and openness of its data and transactions. Lack of uniformity, accessibility, ownership, and change management are some of its drawbacks.

3.2 Screening of Relevant Paper

We next used our search technique to get the articles from the databases and proceeded to evaluate them for relevance. This procedure began with a title-based relevancy check of the publications. We did not use any of the retrieved publications whose titles made it obvious that they had nothing to do with our research. Our search protocol came up several publications, but we had to weed out the ones that didn't pertain to using block chain technology in healthcare. When a paper's relevance could not be judged just by its title, it was sent on to the next round of screening. Abstracts of accepted articles were read in the screening's second round. Some papers didn't make it past our exclusion criteria until we readboth the introduction and the conclusion.

These are some of the things we have to rule out according to our criteria for rejection: Non-peer-reviewed papers (such as press releases and interviews), papers without full text availability, papers whose primary focus is not on the use of block chain technology in healthcare, papers written in languages other than English, papers that have since been retracted, and papers that are duplicates of existing ones.

3.3 Key wording on The Basis of Abstract

The purpose of this procedure was to create a taxonomy of the relevant research articles in the literature. We accomplished this by following the steps shown in Figure from the aforementioned resource. The procedure entails harvesting keywords and ideas from the abstracts of the publications that accurately represent the papers' contributions. These terms were used to classify the papers into several sets. After the articles were first grouped into their respective categories, a closer perusal of each one showed whether it belonged in that grouping, therefore the classifications were revised accordingly. If it is determined that the document does not fall into any preexisting categories, a new category may be developed. The final product of this procedure is an organized list of all therelevant documents that fall under various headings.

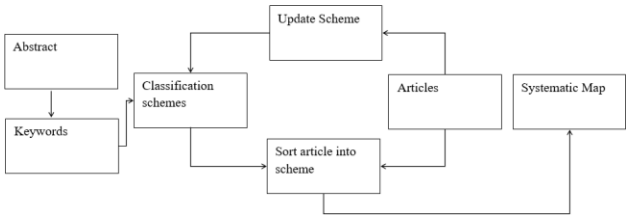

Figure 6. Paper Classification Process

3.4 Data Extraction and Mapping

Finally, we used the information gleaned from the research articles to do a meta-analysis and answer the research questions posed at the outset of the systematic mapping process. As can be seen in Table, ten different pieces of information were culled from each study. Year of publication, title, authors, country of origin (where many writers are involved, the nation of the corresponding author or the first author is utilized), publishing venue, etc. were the first seven elements retrieved. After carefully reading the documents, we were able to collect the remaining data pieces (numbers 8 through 10). In addition to these pieces of information, we also assigned a unique number (between 1 and 65) to each of the chosen articles. For the sake of organizing and analysis, the retrieved data were compiled in an Excel file.

3.5 Effect Size

As blockchain data cannot be altered after it has been recorded, even seemingly innocuous alterations may lead to misleading results. Transactional non-repudiation may be enabled with the use of digital signatures, non-symmetric encryption/decryption technologies, and decentralized consensus mechanisms. Information stored on a blockchain together with its metadata may be utilized to track out where a particular piece of information originated.

Meta-analysis requires effect size calculations for comparison analysis. Effect values show the intensity and type of variable connections. If the impact value and variable relation are positive, bigger effect values should result in a more strong and persistent variable connection. This meta- analytic analysis used correlation coefficients to assess effect sizes, as advised by Hunter and Schmidt. As the included studies employed various measurement methodologies, the correlation coefficient replaced the effect size.

This study's effect was adjusted using the following formula, using the correlation coefficient r as the input variable.

$$r' \quad \frac{r'}{\sqrt{\alpha_{xx}\alpha_{yy}}}$$

Where r 0 is the adjusted correlation coefficient across studies, r is the correlation coefficient (or impact size) across individual studies, xx is the reliability coefficient of the independent variable, and yy is the reliability coefficient of the dependent variable. Strengthening the scale's dependability by modifying the correlation coefficient's attenuation fluctuation. To account for characteristics for which not all studies provided reliability data, we weighted averaged the reliability of related research. Very few trials were like others.

$$\text{Fisher}'s\ Z_i = 0.5 \times \ln\frac{1+r'}{1-r'}$$

$$\text{Fisher}'s\ Z_+ = \frac{\sum n_i Z_i}{\sum n_i}$$

$$r_z = \frac{e^{2 \times \text{Fisher}'s\ Z_+} - 1}{e^{2 \times \text{Fisher}'s\ Z_+} + 1}$$

The formula looks like this: ni = sample size matching to impact value I, where r 0 = correlation coefficient of each study after reliability adjustment.

IV. RESULT AND ANALYSIS

4.1 Statistical Analysis

To find out how much the results from each experiment differ from one another, we must conduct a heterogeneity test. Common statistical tools for investigating the effects of heterogeneity include the Q-value and the I2 value. As the Q- value was significant (p 0.05), this suggests that there is substantial heterogeneity across the studies. I 2values of 25%, 50%, and 75%, respectively, reflect low, moderate, and high degrees of heterogeneity. A random-effects model is utilized, instead of a fixed-effects model, if the distribution of effect values is found to be non-normal. Assuming that all studies included in the meta-analysis use the same

population and give just one estimate of the true amount of the impact, a fixed-effects model creates weight by looking at the variations that exist within the study itself. In other words, the model assumes that any discrepancies in effect size are attributable only to tiny sampling mistakes and not to any differences across studies that may account for them. Conversely, a random-effects model considers both within- study and between-study variances to determine weights. The model assumes that the effect values included in the meta-analysis do not all have the same value and that they change based on variables like subject characteristics, experimental methodologies, etc. This approach also takes into consideration the fact that the effect value computation may be affected by variances across research and by sample mistakes within studies. By estimating the mean value of the effective distribution, a random-effects model may prevent either underestimating the weight of small-sample studies or overestimating the weight of large-sample research. Another advantage of this kind of model is that its mean value may be used to calculate the effective distribution's mean. Based on the findings of the heterogeneity test, the random-effects model was chosen for this study. To find out how much the results from each experiment differ from one another, we must conduct a heterogeneity test. Common statistical tools for investigating the effects of heterogeneity include the Q- value and the I2 value. As the Q-value was significant (p 0.05), this suggests that there is substantial heterogeneity across the studies. I 2values of 25%, 50%, and 75%, respectively, reflect low, moderate, and high degrees of heterogeneity. A random-effects model is utilized, instead of a fixed-effects model, if the distribution of effect values is found to be non-normal. If all studies included in the meta- analysis use the same population and give just one estimate of the true amount of the impact, a fixed-effects model creates weight by looking at the variations that exist within the study itself. In other words, the model assumes that any discrepancies in effect size are attributable only to tiny sampling mistakes and not to any differences across studies that may account for them. Conversely, a random-effects model considers both within-study and between-study variances to determine weights. The model assumes that the effect values included in the meta-analysis do not all have the same value and that they change based on variables like subject characteristics, experimental methodologies, etc. This approach also takes into consideration the fact that the effect value computation may be affected by variances across research and by sample mistakes within studies. By estimating the mean value of the effective distribution, a random-effects model may prevent either underestimating the weight of small-sample studies or overestimating the weight of large-sample research. Another advantage of this kind of model is that its mean value may be used to calculate the effective distribution's mean. Based on the findings of the heterogeneity test, the random-effects model was chosen for this study.

Hypothesis	Pair wise relationship	K	N	Heterogeneity				Tau-squared			
				Q	df (Q	P	I²	Tau squared	Standard error	Variance	Tau
H1	EHR to PI	6	2279	55.890	5	0.000	91.054	0.027	0.019	0.000	0.165
H2	EHR to DS	5	1860	26.983	4	0.000	85.176	0.016	0.013	0.000	0.126
H3	EHR to DM	6	2016	17.557	5	0.000	71.521	0.008	0.007	0.000	0.087

Figure 8. Heterogeneity test

The decentralized, blockchain-based, and industry-standard healthcare management system, with the use of blockchain and connected medical devices, the suggested solution creates a secure and efficient RPM and EHR administration platform. The proposed system architecture incorporates the decentralized storage concept and a permission less blockchain network as an ACP to track a patient's vital signs. Both ideas originated with blockchain computing. Finally, there is a negative relationship between Blockchain in Electronic health record' perception of risk and their intention to make Personal Identity of Patents. When Blockchain in Electronic health record larger probability of bad results, they are more likely to be dubious about and make less of an effort to choose Electronic Health Record System. Consequently, it is crucial for Hospitals to ease Patients' minds so that they would feel more comfortable using electronic health Record good.

4.2 Hypothesis Testing

Hypothesis Testing

Hypothesis	Accepted/ Rejected
Hypothesis 1	Accepted
Hypothesis 2	Accepted
Hypothesis 3	Rejected

Figure 9. Hypothesis Testing

Results from the Meta analysis support the null hypothesis, with the beta value of patient identity being 0.204 and the p value being 0.000 (p 0.05). The beta for Data security is 0.634, and the p value is 0.000 (p 0.05), hence the second hypothesis is also true. The beta value of Data monitoring is 0.004, but the p value is 0.967 (p > 0.05), hence the third hypothesis of the research is not supported.

4.3 Systematic Data Analysis

Symmetric encryption was suggested to organize and distribute electronic medical records for the treatment of cancer patients. Patients may develop their own symmetric encryption keys to protect their data while communicating with their physicians. Clinicians will get a new key in accordance with their organization's set access regulations if the symmetric key is ever compromised, and the data will be re-encrypted using a proxy re-encryption technique in the trustworthy cloud. The security of data exchange may be further improved by using smart contracts to allow only patients to share symmetric keys and establish access rules. With the system developed by [30], users may verify their identities and get access to requested data from a central repository of sensitive data. Membership verification keys and transaction keys are generated via the system's User- Issuer Protocol. When the User-Verifier Protocol is used to check a user's membership status, only authorized users areallowed to submit requests for information.

Using efficient yet lightweight public key cryptography processes, [31] improved the security of approved requests (append, retrieve). As a patient's signature is required to add a transaction to a private blockchain, no one may change a patient's records without first notifying the patients themselves.

This method, developed by [32], integrates Ethereum with attribute-based encryption (ABE) technology with the aim of achieving fine-grained access control over data in a distributed storage system without a trustworthy private key generator (PKG). The key to decrypting the file is encrypted using AES and then added to the distributed ledger. In order to access encrypted files on IPFS, requesters must first get the file encryption key. In addition, the smart contract- implemented keyword search protects against dishonest cloud server behavior.

[33] created a mechanism to improve healthcare data sharing amongst PSN nodes. The healthcare data comes from the WBAN, or wireless body area network (WBAN). PSN nodes may construct secure connections for the WBAN using an improved version of the IEEE 802.15.6 display authenticated association and, if verification is successful, obtain access to exchanging data with other nodes by looking up the addresses of sensors and mobile devices in the blockchain. The data storage capabilities of the PSN nodes and the processing power of the sensors are not significantly taxed throughout this approach. Since everything is saved in the digital gadgetsand the body sensors, there is no chance of data leaking due to criminal activity.

[33] proposed BPDS as a blockchain-based approach to exchanging EMR data in a way that preserves patients' privacy. The system adopted content extraction signature (CES) Steinfeld et al. (2001), which can remove sensitive information of EMRs, support for selective sharing data, and generate valid extraction signatures, to help lessen the possibility of data privacy leakage and to aid in strengthening the security of access control policies. In addition, users may protect their anonymity by generating a new public key for each transaction.

To address the problem of mistrust between parties by relying on a single verifiable signature, Hui et al. (0000) developed a blockchain-based data sharing system in the cloud computing setting. The requestor may use the immutable ledger record to confirm the accuracy of the supplied information. In the event of a disagreement, the group signature will reveal the true identity of the data owner to the organizations responsible for managing the group's participants. Data exchange with audit trails has been shown to improve relationships between companies.

An EHR model was presented by Seol et al. (2018) that implements attribute-based access control using XACML, an extensible access control markup language with the flexibility to design rules for a variety of use cases. As further precautions against data leakage following the access control stage, we use XML encryption for partial data encryption andXML digital signature for digital signing.

4.4 Proposed model

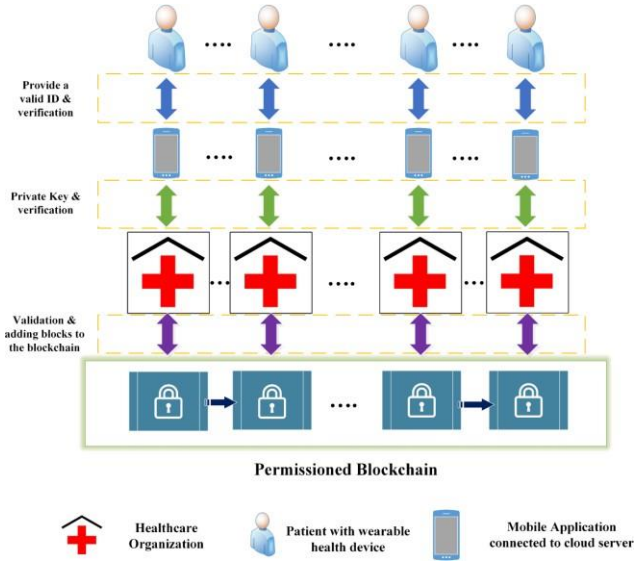

Figure 10. Blockchain network of the proposed model

By getting and operating the data with previous studies we have come to an end that, the blockchain network, the consensus method, and the system architecture are the three essential factors to think about while analyzing this instance. Our blockchain network will be used to store information such as requests, rules, and data states to ensure privacy and consistency, in addition to the logs of records of medical information when transactions are done and aggregated into blocks. Permission blockchain's, which provide granular control over data access for individually recognizable users, will be utilized in our approach. Permission blockchain improves network speed and security, while also decreasing the cost and workload process for nodes that aren't taking part in the mining process and instead simply do the required calculations for a given application. A patient-entity connection is represented by each transaction. The patient may use a mobile app to look for the record's unique identifiernumber. In Figure 7 you can see how our blockchain networkis proposed.

This thesis proposes a blockchain deployment solution that's both affordable and robust. With the help of systematic and Meta Analysis of previous studies, the suggested blockchain architecture Healthchain has been successfully developed. It ensures the correct operation of the system during transaction execution. In addition, unlike a traditional transaction flow, the implementation of the framework does not appoint an ordering authority to create the block; rather, the process chooses peer pairings that support a more computationally complex task. Health data are protected against unauthorized access thanks to the access control authorization restrictions included in the business network definition (.bna file) and the smart contract implementation that stores EHR transactions as immutable hash values in the Healthchain network. This prototype's use of cryptographic encryption to safeguard data helps guard against malicious intrusions that may compromise a patient's privacy.

V. DISCUSSION

The limits of the study, potential future research avenues, and the broader research effect in the subject of cyber security, which serves as a summary of the significant contributions of the study. There are measures for protecting privacy in the e- health cloud, but they are not sufficient to guarantee complete confidentiality. Internal assaults by people with authorized credentials inside an organization to access data, such as the database administrator or the key manager, pose the greatest threat to electronic health records stored in the cloud and are much more severe than foreign attacks. The risk of data breach or abuse is exacerbated by the fact that information is accessible to cloud service providers. This situation prompted the author of this thesis to design a novel method that provides enhanced security for the e-healthcare system. While the current system has its flaws, our blockchain technology, Healthchain, mitigates these issues by allowing for efficient scaling of electronic health records and safe information exchange throughout the e-health ecosystem. More and more cyber-attacks are having a devastating effect on the healthcare industry. Criminals and cyber threat actors are looking for ways to take advantage of the vulnerabilities that come with the advancements in healthcare technology that are being made to give life-critical services while also improving treatment and patient care. Malicious software that compromises systems and patients' privacy is only one example; distributed denial of service (DDoS) assaults may also impede a healthcare facility's capacity to treat patients. Cyberattacks, such as Ransom wares, may have far-reaching consequences for healthcare organizations, including but not limited to

financial loss and privacy leaks. Patients' confidentiality was another goal of this study, which included making the system more impenetrable to outsiders to forestall any data theft or loss. The study's overarching goal was to create a new task-based framework for data sharing on EHD database federations, one that safeguards data from external and internal threats and gives medical professionals and government resource managers and politician's access toreal-time, visual data. These are the specific aims of the research project:

1) Help fund studies in the medical field. For example, when health data are exchanged or accessed by stakeholders, a framework should be put in place to determine how certified blockchain apps might help manage privacy and protection. Introduce a safe repository for data and come up with a cryptographic way to keep it safe and accessible.

2) Create a system that can better defend users' personalinformation from both internal and external threats.

VI. CONCLUSSION

The most fundamental right of any citizen in any country is the right to privacy, and because e-health data contains a wide variety of sensitive and confidential information, from patient data to financial information like social security numbers andcredit card detail.

Given the importance of personal privacy, there is a pressing need to prevent unauthorized access to sensitive information. Most of the information is very private, making security a top priority. Data and patient confidentiality are protected in thisstudy.

Healthchain, the planned blockchain architecture, is now live on Hyperledger Fabric. The proposed framework constructs chaincode implementations known as smart contracts. The framework's implementation selects peer pairings that can handle a more computationally difficult task. Health data are protected against unauthorized access thanks to the access control authorization restrictions included in the business network definition (.bna file) and the smart contract implementation that stores EHR transactions as immutable hash values in the Healthchain network.

VII. FURURE WORK

Healthchain opens a wide variety of study avenues. For instance, a healthcare provider and a hospital may join forces to build a blockchain network that can transfer data instantly and provide straightforward two-way communication between the two. Block verification is another area that might be thought of as potential future work.

Digital Asset Modelling Language (DAML) is a modeling language for digital assets, as the name suggests; future development will include including support for different databases and ledger technologies, our work will better support medical research and government healthcare resource allocation.

REFERENCES

[1]. Chenthara, S., Wang, H., and Ahmed, K. (2018). Security and privacy in big data environment.

[2]. Punithasurya, K. and Jeba Priya, S. (2012). Analysisof different access control mechanism in cloud. International.

[3]. Kruse, C. S., Mileski, M., Vijaykumar, A. G., Viswanathan, S. V., Suskandla, U., and Chidambaram, Y. (2017a). Impact of electronic health records on long-term care facilities:Systematic review. JMIR medical informatics, 5(3)

[4]. Griebel Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M. Blockchain Utilization in Healthcare: Key Requirements and Challenges. In Proceedings of the IEEE 20th International Conference on e-Health Networking, Applications and Services, Ostrava, Czech Republic, 17–20 September 201

[5]. Abbas, A. and Khan, S. U. (2014). A review on the state-of-the-art privacypreserving approaches in the e-health clouds. IEEE Journalof Biomedical and Health Informatics, 18(4):1431–1441.

[6]. Matturdi, B., Zhou, X., Li, S., and Lin, F. (2014). Big data security and privacy: A review. China Communications, 11(14):135–145.

[7]. Chenthara, S., Ahmed, K., Wang, H., and Whittaker, F. (2019). Security and privacy- preserving challenges of e-health solutions in cloud computing. IEEE access, 7:74361– 74382.

[8]. Ahmed, M. and Ullah, A. S. B. (2017). False data injection attacks in healthcare.

[9]. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Rolebased access control models. Computer, 29(2):38–47.

[10]. Yi, X., Miao, Y., Bertino, E., and Willemson, J. (2013). Multiparty privacy protection for electronic health records. In Global Communications Conference (GLOBECOM), 2013 IEEE, pages 2730–2735. IEEE

[11]. Kruse, C. S., Mileski, M., Vijaykumar, A. G., Viswanathan, S. V., Suskandla, U., and Chidambaram, Y. (2017a). Impact of electronichealth records on long-term care facilities: Systematic review. JMIR medical informatics, 5(3)

[12]. Griebel, L., Prokosch, H.-U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., Engel, I., and Sedlmayr, M. (2015). A scoping review ofcloud computing in healthcare. BMC medical informatics and decision making, 15(1):17.

[13]. Wei, J., Liu, W., and Hu, X. (2016). Secure datasharing in cloud computing using revocable- storage identity-based encryption. IEEE Transactions on Cloud Computing

[14]. Abbas, A. and Khan, S. U. (2014). A review onthe state-of-the-art privacypreserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics, 18(4):1431–1441.

[15]. Zhang, R. and Liu, L. (2010). Security models and requirements for healthcare application clouds. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pages 268–275. IEEE.

[16]. Fuentes, M. R. (2017). Cybercrime and other threats faced by the healthcare industry. Trend Micro.

[17]. AbuKhousa, E., Mohamed, N., and Al-Jaroodi, J. (2012). e-health cloud: opportunities and challenges. Future Internet, 4(3):621–645.

[18]. McGraw, D. (2013). Building public trust in uses of health insurance portability and accountability act de-identified data. Journal of the American Medical Informatics Association,20(1):29–34.

[19]. Li, P., Guo, S., Miyazaki, T., Xie, M., Hu, J., and Zhuang, W. (2016a). Privacy preserving access to big data in the cloud. IEEE Cloud Computing, 3(5):34–42.

[20]. Xue, K., Xue, Y., Hong, J., Li, W., Yue, H., Wei, D. S., and Hong, P. (2017). Raac: Robust and auditable access control with multiple attribute authorities for public cloud storage. IEEE Transactions on information Forensics and Security, 12(4):953–967.

[21]. Wei, J., Liu, W., and Hu, X. (2016). Secure datasharing in cloud computing using revocable- storage identity-based encryption. IEEE Transactions on Cloud Computing

[22]. Li, W., Liu, B. M., Liu, D., Liu, R. P., Wang, P., Luo, S., and Ni, W. (2018). Unified fine- grained access control for personal health records in cloud computing. IEEE journal of biomedical and health informatics

[23]. S. B. C. Wah, P. Welinder, P. Perona, and S. Belongie. The Caltech-UCSD Birds-200-2011 Dataset," California Institute of Technology.

[24]. Mahboob, T., Zahid, M., and Ahmad, G. (2016). Adopting information security techniques for cloud computing—a survey. In 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), pages 7–11. IEEE.

[25]. Choudhury, A. J., Kumar, P., Sain, M., Lim, H., and Jae-Lee, H. (2011). A strong user authentication framework for cloud computing.In 2011 IEEE Asia-Pacific Services ComputingConference, pages 110–115. IEEE

[26]. Kamara, S. and Lauter, K. (2010). Cryptographic cloud storage. In International Conference on Financial Cryptography and Data Security, pages 136–149. Springer

[27]. Chenthara, S., Wang, H., and Ahmed, K. (2018). Security and privacy in big data environment.

[28]. Chi, P.-W. and Lei, C.-L. (2018). Audit-free cloud storage via deniable attributebased encryption. IEEE Transactions on Cloud Computing, 6(2):414–427.

[29]. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53:65–78.

[30]. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. *IEEEAccess* **2017**, *5*, 14757–14767.

[31]. Griebel Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M. Blockchain Utilization in Healthcare: Key Requirements and Challenges. In Proceedings of the IEEE 20th International Conference on e-Health Networking, Applications andServices, Ostrava, Czech Republic, 17–20 September 2018

[32]. Li, W., Liu, B. M., Liu, D., Liu, R. P., Wang, P., Luo, S., and Ni, W. (2018). Unified fine- grained access control for personal health records in cloud computing. IEEE journal of biomedical and health informatics

[33]. Zhu, L., Zhang, C., Xu, C., Liu, X., and Huang,

[34]. C. (2018). An efficient and privacy-preservingbiometric identification scheme in cloud computing. IEEE Access, 6:19025–19033. NIPS, pp. pp. 6629–6640, 2017.