Received 15 June 2022, accepted 3 August 2022, date of publication 11 August 2022, date of current version 19 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3198094

RESEARCH ARTICLE

PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms

KIRTIRAJSINH ZALA[1], (Graduate Student Member, IEEE), HIREN KUMAR THAKKAR[2], RAJENDRASINH JADEJA[3], PRIYANKA SINGH[4], KETAN KOTECHA[5], AND MADHU SHUKLA[1]

[1]Department of Computer Engineering, Marwadi University, Rajkot, Gujarat 360003, India
[2]Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, Gandhinagar, Gujarat 382007, India
[3]Department of Electrical Engineering, Marwadi University, Rajkot, Gujarat 360003, India
[4]Department of Computer Science and Engineering, SRM University—Andhra Pradesh, Amaravati 522502, India
[5]Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune 412115, India

Corresponding authors: Hiren Kumar Thakkar (hiren.thakkar@sot.pdpu.ac.in) and Ketan Kotecha (head@scaai.siu.edu.in)

This work was supported in part by the Symbiosis International University, Pune, India.

ABSTRACT In the current digital era, personal data storage on public platforms is a major cause of concern with severe security and privacy ramifications. This is true especially in e-health data management since patient's health data must be managed following a slew of established standards. The Cloud Service Providers (CSPs) primarily provide computing and storage resources. However, data security in the cloud is still a major concern. In several instances, Blockchain technology rescues the CSPs by providing the robust security to the underlying data by encrypting data using the unique and secret keys. Each network user in Blockchain has its own unique and secret keys linked directly to the transaction keys as a digital signature to protect the data. However, Blockchain technology suffers from the latency and throughput issues in high workload scenarios. To overcome e-healthcare records privacy issues in a third-party cloud, we designed a Patient's E-Healthcare Records Management System (PRMS) that focuses on latency and throughput. A comprehensive performance analysis of PRMS is carried out on different third-party clouds to validate its applicability. Moreover, the proposed PRMS system is compared with Blockchain platforms such as Hyperledger Fabric v0.6 and Etherium 1.5.8 against latency and throughput by adjusting the workload for each platform up to 10,000 transactions per second. The proposed PRMS is compared to the Secure and Robust Healthcare-Based Blockchain (SRHB) approach using Yahoo Cloud Serving Benchmark (YCSB) and small bank datasets. The experimental results indicate that deploying PRMS on Amazon Web Services decreases System Execution Time (SET) and the Average Delay (AD) time by 2.4%, 8.33%, and 25.15%, 15.26%, respectively. Additionally, deploying PRMS on the Google Cloud Platform decreases System Execution Time (SET) and Average Delay (AD) by 2.27%, 2.4%, and 2.72%, 4.73% AD, respectively. The experimental results confirm the superiority of the PRMS under the high workload scenario over SRHB and its applicability in cloud data centers.

INDEX TERMS Cloud computing, e-health, privacy, information security, blockchain.

I. INTRODUCTION

In the current era of digital communications, data are preferred to be stored in the cloud data centers over the local systems. Data generated from state-of-the-art applications such as Smart city, Internet of Medical Things (IoMT), E-healthcare are stored and process on the cloud platforms owned by Cloud Service Providers (CSPs). However, CSPs merely provide the storage, and data processing infrastructure and do not provide comprehensive data security framework.

The associate editor coordinating the review of this manuscript and approving it for publication was Dian Tjondronegoro.

In several instances, CSPs integrate the third-party security framework for privacy preservation and data protection. However, third-party security frameworks are subject to integration issues and expensive. On the contrary, Blockchain technology provides confidence and transparency by delivering immutable blocks of chain. The Blockchain enabled solutions make the most obvious answer for preventing data tampering without relying on third parties in an environment where cloud security is easily accessible. However, Blockchain enabled security has shortcomings while processing multiple transactions such as latency and throughput. In the proposed work, we have exclusively focused to improvise the latency and throughput during the multiple transactions scenarios arise during the access of E-healthcare Records (EHRs).

Electronic records can integrate information from many registered resources and provide a more comprehensive picture of exact patient details, even though this has proven to be a challenging task [1]. Healthcare data is at great risk due to the cloud, despite all of its advantages over on-premises storage. The healthcare sector is undergoing a change as paper-based records are being phased out and replaced by computerized ones [2]. Personal Health Records (PHR), Electronic Health Record (EHR), Electronic Medical Records (EMR), and Electronic Health Data (EHD) are examples of digitalized electronic medical records that have evolved from paper-based records. EHR and EMR refer to patient health records maintained by healthcare professionals, whereas PHR refers to regularly maintaining and monitoring personal information by the patient or their relatives. EHD, also known as electronic health records or computerized patient records, is a type of smart health record that is delivered to patients [3]. Medication, medical histories, demographics, immunization records, laboratory test results, and other confidential patient information are all contained in these records. Traditional paper-based records have considerable disadvantages when compared to EHD systems. Compared to paper-based records, EHR involves less human resources, time, and physical storage [4].

Due to data centralization on the cloud, consumers and healthcare providers have several security and privacy issues. (1) Provides an all-in-one honeypot for attackers to steal information and exploit transmitted data, and (2) transfers ownership rights to cloud service providers, allowing individuals and health care professionals to lose control of confidential data [5]. Recent developments in virtualization technology have enabled users to manage cloud data center computing, and networking resources for e-healthcare data [6], [7]. Cloud-assisted health care delivery system is designed for patient's health care records for efficiency, scalability, and performance improvement [8]. Many proposed Blockchain systems use privately owned Blockchain and open-source platforms such as Ethereum. Blockchain has huge potential for securing health care systems and patient health records in a cloud environment [9]. Patients today require a sophisticated and advanced smart healthcare framework suited to their health requirements due to new technologies and the rapid advances in human life. In [10], the authors have presented a summary of the general application of IoT solutions in edge platforms for medical treatment and healthcare. Furthermore, the current tendency is to use a cloud environment to share and manage massive amounts of distributed medical data, including EHR and lab test results, throughout the e-health system. Cloud storage services offer a viable and scalable solution to such massive data management challenges [11], [12], [13], and [14].

Patients must be able to grant authorized individuals selective, partial, or total access to their data. This is known as consent management, and it is a critical issue in e-Health [15]. Several method like the Least Significant Bit (LSB) method of data steganography uses 8 pixels from the image to hide one character of the secret message. Each binary bit from the private message character is added to the least significant bit of the corresponding pixel in the image. Steganography's Least Significant Bit (LSB) technique replaces an image's least important bit with a bit of data (a byte has 8 bits, and the least significant bit number is 8) [16]. Using a physical object or another piece of data to cover up data is known as steganography [16]. New steganographic methods like null ciphers, picture coding, audio, and video [16] is being used in the advancement of technology. Blockchain is a technology that revolutionizes the concept of trust in next-generation systems. It promotes the idea of conducting any transaction without a mediator.

Mediators, such as businesses and governments, are almost always centralized entities that receive, process, and store transactions. All of the faith that we, as users, place in a system is placed in the mediators who are obligated to process transactions using the correct business logic. The mediators have complete control over data security and privacy. In Blockchain-based systems, trust is decentralized. Users only need faith in the system and the shared smart code among all participants. Thanks to Blockchain, data and transactions are now stored and recorded in a completely new way. The idea behind a Blockchain is to eliminate the middleman, which is similar to a traditional database [17]. The first use of Blockchain technology was in 2008 when proposed the concept of a digital currency called Bitcoin.

Despite the numerous benefits of this technology, migrating to the cloud presents several challenges. In this regard, security and privacy are the main hindrances to the widespread adoption of medical records processing through the use of cloud computing. The third-party provider has complete control over the shared infrastructure model as shown in Figure 1. The Cloud Service Providers (CSPs) are the ones that control the services for this type of cloud system. As Figure 1 depicts, Electronic Health Records (EHRs) are often shared between different entities. Because EHRs are kept on servers outside of the hospital controlled by CSPs, they are very open to attacks and modification. We need good cryptographic tools and fine-grained access control frameworks in third-party clouds to get over this security problem.

The research goal in this paper is to improve the security of e-healthcare records in cloud computing environments and keep their privacy by reducing the number of security and privacy problems in cloud computing, such as information loss, data modification, and data leaks. So, the following points are the contribution and main focus of this study:

1) A presentation of a secured Patient's Medical e-healthcare Records Management System (PRMS) hosted on the cloud provided by a third-party service provider.
2) Implementation of a cloud-based, customized steganographic encryption system for storing electronic healthcare records using a web application prototype hosted on a third-party cloud service provider.
3) Implementation of a cloud-based, customized steganographic encryption system for storing electronic healthcare records using a web application prototype hosted on a third-party cloud service provider.
4) The proposed PRMS approach is compared to the SRHB approach in terms of system execution time and average delay.
5) Design a communication and data acquisition model for distributed e-healthcare scenarios in a cloud environment.
6) Etherum and Hyperledger Fabric have never been compared to any other cloud platform.
7) Main performance matrices include user transactions counted, latency, and throughput.

Both Electronic Medical Records (EMRs) and Electronic Health Records (EHRs) are highly crucial to the long-term vision of healthcare digitization for enhancing patient safety, quality, and efficiency and lowering healthcare delivery costs. Laboratory information systems, Electronic Health Records (EHRs), pharmaceutical information systems, and medical imaging can benefit from cloud storage, management, security, sharing, and archiving. Overall, patients will receive good care due to up-to-date health records and constant interactions with numerous healthcare professionals. A third-party cloud has several security challenges and concerns like any IT program. Because it often operates in an open and shared environment, it is prone to data loss, theft, and malicious assaults. A scarcity of cloud security is one of the primary roadblocks to complete cloud adoption in the healthcare business. The difficulty in surrendering control over their medical records is one of many reasons why healthcare professionals fear the cloud. Cloud providers often preserve their data in several different data centers around the globe. Data stored around the globe is an obvious benefit because cloud data storage would be redundant, multiple data centers will assist in the event of a calamity, and disaster recovery is an enormous advantage. On the other hand, this same benefit could be a security risk because data kept in different places are more likely to be stolen or lost. EHR is usually private and confidential because they have patient identifiers and very sensitive information. Users who use cloud computing services, on the other hand, don't have physical control over their data. Furthermore, cloud service providers cannot be trusted entirely. Due to a lack of transparency, it is difficult to know where, how, and when data is handled, making it difficult to verify the service provider, resulting in catastrophic data loss. So users cannot fully trust third-party cloud service providers while storing health records. Double-layer security is required to secure the privacy and security of e-health records stored on a third-party cloud.

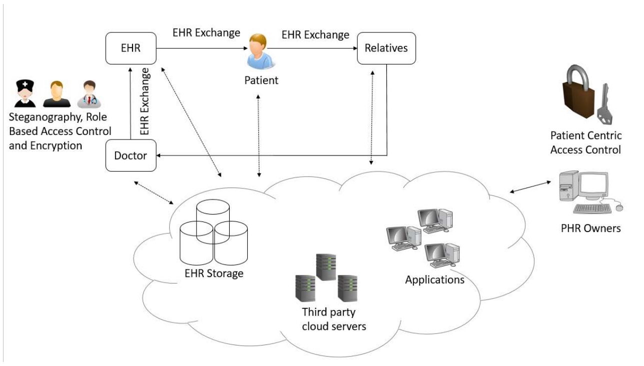

EHR Exchange
EHR Exchange
EHR
Patient
Relatives
Steganography, Role Based Access Control and Encryption
EHR Exchange
Doctor
Patient Centric Access Control
PHR Owners
EHR Storage
Applications
Third party cloud servers

FIGURE 1. High-level general overview of cloud-based electronic health records.

The remaining sections are as follows: Section 2 discusses the Related Work, Section 3 describes the proposed PRMS System, Section 4 explains the PRMS system design implementation, Section 5 presents the experiments setup with results and discussion, and Section 6 ends with the conclusion.

II. RELATED WORK

This research examines a wide range of databases, including IEEE, Google Scholar, Science Direct, Springer, Elsevier, Scopus, and ACM to find alternatives to cloud-based EHRs that preserve security and safety. Public, community, private or hybrid cloud can be the e-health cloud architecture. Depending on the personal data, access control methods are necessary because EHR data is highly confidential, contains sensitive patient information, and is stored on third-party servers. Access control is a protective shield that restricts the operation of the public health system and access to medical records in order to preserve the privacy of that information. Security measures in healthcare facilities are typically implemented using Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC). ABAC [18] uses both cryptographic and non-cryptographic approaches, whereas Identity-Based Access Control (IBAC) uses Identity-Based cryptographic methods that encrypt data using the user's identity. The author's research in paper [19] resulted in a patient-centered monitoring system that reduces the risk of storing and retrieving electronic health data on the cloud. This study develops a system that allows patients to choose how and when their health data is retrieved, either directly or indirectly. Public key encryption and hash values are used to encrypt health records. In, paper [20] includes Universal Designated Verifier Signatures (UDVS), which generate an assigned verification signature and guarantee that patient data utilization is restricted to authorized entities. Since the health data is generated directly by an issuer who fully understands the details of the record, hash values, and signatures, the method's primary disadvantage is that the confidentiality of the record is put at risk [20]. A personal health information system which the author utilizes the system from various angles to secure the Personal Health Information (PHI) by employing asymmetric key cryptography and message digest. Furthermore, the author uses attribute-based broadcast encryption [21]. A multi-layered accessing delegation, including attribute revocation methods, is possible with this technology. In smart health systems, an authentication algorithm and RBAC are often used to secure patient privacy [22], the health board, healthcare experts, and the information consumer all are involved. The author presents a scheme for recommending online medical services to e-healthcare users while protecting their privacy to help them find an appropriate physician [23]. Author [24] presented two RBAC strategies for EHR, one for patients and the other for medical personnel. Patients are identifiable by their identities, while their responsibilities define the medical staff, and access is provided according to access policies. This strategy also offers revocation procedures for users. Blockchain technology [25] can be utilized to enable this distributed ledger approach in the cloud, an underlying access control tool. In the cloud, a secure Blockchain-based EHR solution, smart permission agreements, or written codes that validate data ownership, permissions, and integrity are known as smart contracts. As hash values are used to store all health transaction information in the Blockchain, this method is tamper-proof. It has significant potential to improve e-health data security, complexity, confidentiality, availability, and integrity. With the help of cryptographic features, this new technology makes it safe and easy to store, transfer, and access electronic health records in the cloud [26]. Because of its importance in overcoming the interoperability and security challenges of EHR and EMR systems in e-health, Blockchain technology has experienced a massive boom in the health sector. There are considerable challenges ahead before Blockchain can live up to its potential and be used in medical care. The most critical challenges are technology scalability and data access control [27]. In the paper, [28] a system that only works on the Bitcoin and Ethereum platforms for data analytics is presented. The suggested model in a recent study integrates comparative Blockchain data with data from different sources. It can also assemble data in a database using the framework. A recent paper studied quality concerns, ideas, and needs for Blockchain deployment and identified the quality characteristics of Blockchain technology [29]. Blockchain platforms need to be enhanced in various areas, including security, flexibility, opacity and performance in terms of latency, cost-effectiveness and other considerations, according to the research [29]. The research in paper [30] tries to forecast the latency of Blockchain-based systems using a simulation system and performance modeling. The relative error for the majority of the predicted results is less than 10%. This approach also aims to aid in the evaluation of various Blockchain design alternatives. Although Blockchain technology in e-health has many benefits, it also has some drawbacks. Risks were classified into three categories in this review: technological, cultural, and organizational threats. Scalability, approval, security measures, high power and energy consumption have been the main technological challenges. Scalability has become a significant challenge to public Blockchain applications due to the lack of control over the number of people entering the network [31]. Furthermore, because the data created by these sensors develops at an exponential volume, challenges arise when connecting wearable devices to Blockchain networks challenging to manage [32]. Moreover, the Blockchain network is vulnerable to cyber-attacks that disrupt, halt, or reverse previously authenticated transactions within the network, which can result in disaster. Furthermore, because it is related to proof-of-work-based Blockchain, this review identified excessive energy consumption as a risk (public Blockchain). This mining method requires a significant amount of energy. The number of transactions per second has increased as more people join the Blockchain network [33]. Another primary social concern was the lack of judicially enacted Blockchain technology legislation. These regulations have been hampered by decentralization and the disconnection of trusted third parties. Meanwhile, interoperability concerns, a lack of technical expertise for integrating pharmaceutical suppliers, installation, and transaction costs were the most common organizational threats. Interoperability has been identified as a significant barrier to Blockchain technology adoption in healthcare, owing to a lack of confidence between healthcare organizations and a scarcity of IT professionals available to implement Blockchain technology. Insufficient technical knowledge and competencies may be serious when it comes to using Blockchain technology [31], [34]. Using a consortium Blockchain, author [35] proposes an ABSE (Attribute-Based Searchable Encryption) scheme for healthcare CCPS (Cloud-based Cyber-Physical System) that is decentralized, robust, and computationally efficient. A typical CCPS in healthcare utilizes devices with limited resources. The author describes the proposed cloud infrastructure and conducts an analysis of it using mathematical models to produce significant diagrams about a variety of metrics [36]. The author discusses an algorithm that can be used to improve Cloud Computing security by using algorithms that can provide more privacy in Big Data technology-related data [37]. Lightweight architecture and the associated protocols for consortium Blockchain-based identity management are proposed in this paper. The aim of the paper [38] is to address issues relating to privacy, security, and scalability in a centralized system for the Internet of Things (IoT). Author [39] suggests a new model in which a permission Blockchain would be used to manage and store the Electronic Health Records (EHR) of patients who have registered with the system. Transparency and immutability are critical for secure administration and storage, and this system assures that both doctors and patients can rely on it with confidence, thus restoring public confidence in the health care system as a whole. This system also provides secure management and storage of sensitive information. The author [40] conducts a survey of the field of brain tumor MRI image segmentation in this particular paper. In addition, the author provides a summary of multi-modal brain tumor MRI image segmentation methods. The author discusses the cyber syndrome in this paper [41]. Cyber syndrome is a collection of physical, mental, and social disorders that can occur when individuals excessively spend too much time in cyberspace and connect to it. At this point, the focus is on identifying future indicators of privacy and security in Electronic Heath care Records (EHRs). Data stored on third-party servers, such as EHRs, pose significant risks to privacy and security because of the sensitive nature of the information. Major research issues include the following:

1) The use of confidential health care data.
2) To protect data, what is the best encryption method?
3) Using data storage protection, how can we ensure the security of our medical records?
4) How can patient's health information be easily shared among various medical practitioners?
5) In the event of a medical emergency, who will have access to a patient's medical record?

Various privacy and security concerns for e-health information are brought to light in the preceding points. As a result, we have analyzed and identified the need for e-health systems to use security infrastructure protecting patient privacy and trust over the third-party cloud.

TABLE 1. Notations.

Notations	Meaning
EHR	E-Healthcare Record
$PRMS$	Patient Records Management System
D	Set of Doctors
P	Set of Patient
R_k	Set of Relatives
Z_j^i	Set of E-Health Records access rights of i^{th} patient to j^{th} doctor
κ	Set of relative sets
E	Set of E-Health records
ζ_j^i	Access rights of i^{th} patient to j^{th} doctor
d_j^i	j^{th} Doctor has access of i^{th} patient
p_j^i	i^{th} Patient associated with j^{th} doctor has EHR access.
T	Time Frame for patient monitoring data in system
DC_y	Number of geo-distributed data centre located in cloud
DW_x	Number of Gateways
c	Frequency of consultation
w	Window intervals
ψ_c	Probabilities of patients consultation frequency
ψ_d	Probabilities of patients consultation frequency to doctor
ψ_v	Least value of patient consultation to doctor
ρ	Number of different degree of different doctors registered in PRMS in system
Δ	Data computation
ξ	Data in size of mega bytes
η^p	Aggregated data generated by Patient p
$\eta^p_{\tau\alpha_i}$	Text Data of Patient p
$\eta^p_{\tau_\beta j}$	Report of Patient p
g	Text documents
z	Image documents
σ	Rate of active server
$\wp$	Data allocation types
Ω	Active Servers
$H_{p,g}$	Incoming rate of data from patient to gateway
$\wp_s^d$	Short processing type data
$\wp_\Lambda^d$	Delay processing type data
$\wp_{pr}^d$	Prioritised data
$\wp_{po}^d$	Posteriority data
$\phi^p(w)$	Amount of data collected from a patient p

III. PROPOSED PRMS SYSTEM

A. COMMUNICATION MODEL

The communication model of the proposed PRMS system is shown in Figure 2. There are three entities in our cloud-based communication model: patients, doctors, and relatives. Here, patient records are considered as E-Health Care Records (EHRs), which are stored in the third-party cloud platform such as AWS(Amazon Web Service), and GCP(Google Cloud Platform) and retrieved as per the requirement using a web-based application. The cloud-based healthcare environment is explained as follows. Let D be a set of n doctors denoted as $D = \{d_1, d_2, \ldots, d_n\}$, where $n > 0$. Let P be a set of m patients denoted as $P = \{p_1, p_2, \ldots, p_m\}$ where $m > 0$. Let κ be a set of m subsets denoted as $\kappa = \{R_1, R_2, \ldots, R_i\}$. Here, each subset $R_i \in \kappa$, It represents the set of k relatives associated with each patient $p_i \in P$. The set of relatives associated with each patient $p_m \in P$ is represented as $R_i = \{r_{i1}, r_{i2}, \ldots, r_{ik_i}\}$. For any patient $p_i \in P$ there exist a corresponding $E_i \in E$, where $i = \{1, 2, 3, \ldots, n\}$ and $E = \{e_1, e_2 \ldots e_h\}$. Doctors may have access to the patient's E-Healthcare Records given by the patient, let Z_j^i denotes the E-Healthcare Records access of $p_i \in P$ to doctor $d_j \in D$, where $e_1 \in E$, E denotes set of patient's E-Health Care Records. Access can be represented as $Z_j^i = \{\zeta_1^2, \zeta_2^2 \ldots, \zeta_j^i\}$ where $m =$ number of patient for access rights of i^{th} patient to j^{th} doctor. To enhance quality of patient monitoring, the entire time span T is divided into multiple windows denoted as $T = \{0, 1, 2 \ldots .t\}$. Consider the underlying healthcar application, the timeline are generalized as minute, hour, week, or year. Accordingly $P_m =$ Patient and $D_n =$ Doctors volume of data generated collected data stored in different cloud data centre. Let $\{DC_1, DC_2 \ldots .DC_y\}$ be the geographically distributed cloud data centers, these data centres are linked via series of x number of gateway $G = \{GW_1, GW_2 \ldots GW_x\}$. In our communication model P and D numbers of patient and doctors linked with these y numbers of geographically distributed cloud data centers through x numbers of gateways through web-application [42]

B. DATA ACQUISITION MODEL

Traditional healthcare systems collect, store, and process patient data, making it impossible to diagnose complex health issues. In comparison, the proposed PRMS data acquisition model considers all stakeholders, as data generation sources, based on a patient's frequency of consultation (c), whereas existing schemes only consider the number of patients. To improve the effectiveness of patient monitoring,

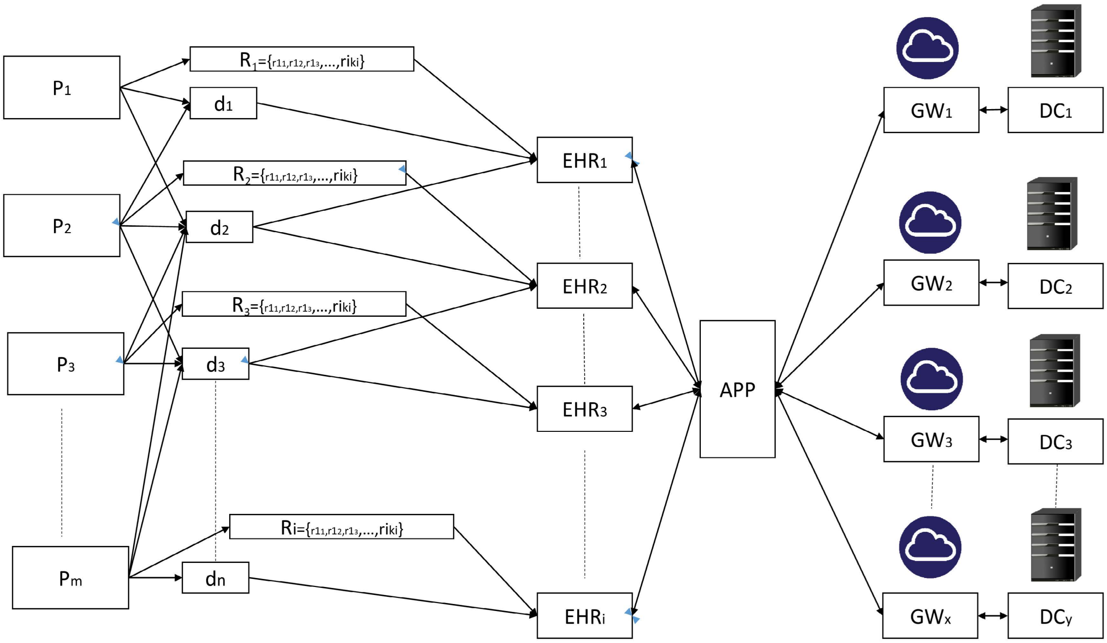

P1
P2
P3
Pm
R1={r11,r12,r13,...,riki}
d1
R2={r11,r12,r13,...,riki}
d2
R3={r11,r12,r13,...,riki}
d3
Ri={r11,r12,r13,...,riki}
dn
EHR1
EHR2
EHR3
EHRi
APP
GW1
GW2
GW3
GWx
DC1
DC2
DC3
DCy

FIGURE 2. Communication model for the proposed PRMS system.

a window-based temporary information gathering and monitoring methodology is applied. Depending on the health issue or requirements, the size of the window could be adjusted. Self-monitoring and time series patients are usually more effective for those who have their state-monitored based on health-related parameters. The number of patient-doctor consultations must be analyzed, as data is collected during each consultation via a cloud-based e-health application. Let assume patient (p_m) consult doctor c times through our cloud-based PRMS e-health application within the w timelines. At the time of each patient's consultation, let ψ_c, ψ_d be the probability of the patient's consultation frequency to doctors in any window timeline w. It must be observed that ψ_v is the least value of patients who consult doctors.

Theorem: Probability of consultation ψ_v of a patient to doctor is at least $\frac{c}{d\rho_w}$.

Proof: Let us consider that c is the frequency of consultation of patient with doctor p^i_j to i^{th} patient to j^{th} doctor.if there are d be the number of doctors registered in PRMS system and ρ be number of different degree of different doctors registered in PRMS in system with in window w. Hence probability of frequency of consultation and uploading EHRs on cloud server is ψ_c of patient to doctor with in window w can be expressed as $\frac{c}{w}$. Total Probability of cosultation can be expressed as: $\psi_v = \psi_c \times \psi_D$. if we proceed further ψ_v can be $\frac{c}{w} \times \frac{1}{\sum_{i=1}^{d} D_i}$. ψ_v becomes $\frac{c}{d\rho_w}$. It should be observed that the likelihood of consulting a doctor via the cloud and uploading EHR grows monotonous with c and w. In the proposed model for the data acquisition scheme, we consider both text and patient reports uploaded to a cloud server via a PRMS e-health application hosted on a third-party cloud server. In our data allocation model, data is assigned with respect to computation (Δ) and (ξ) megabytes represent the size of each text and patient report uploaded on a cloud server through an e-health application and η^p represent the amount of data generated by patient p during a single consultation. Thus η^p is aggregated amount of both text ($\eta^p_{\tau\alpha_i}$) and patient report ($\eta^p_{\tau\beta_j}$) EHR of patient p, which can be expressed in given Eq. 1.

$$\eta^p(w) = \sum_{i=1}^{g}(\eta^p_{\tau\alpha_i})(w) \times \Delta + \sum_{j=1}^{z}(\eta^p_{\tau\beta_j})(w) \times \xi \tag{1}$$

where η^p is data generated in window w, g and z are the numbers of text and patient reports in the e-health application system. For patient p in single consultation window w considering consultation probability of patient, the amount of data collected from the patient can be written as $\phi^p(w)$ can be expressed in given Eq. 2.

$$\phi^p(w) = \eta^p(w) \times \psi_v(w) \tag{2}$$

C. MODEL FOR DATA ALLOCATION

Our data allocation model considers the active server computation rate (σ) and data allocation types ($\wp$). It is considered that data processing in data centers is rapid with no buffering or queuing delays. Prior to data execution, the data is distributed with multiple replicas across many of the data center's active servers (Ω) which used to reduce network congestion, increase computational throughput, and enhance network efficiency. Our designed system considers incoming data in two stages from the patient to the gateway as well as from the gateway towards the data center's active servers, let $H_{p,g}(w)$ be the data incoming rate from $p \in P$ to $g \in G$ in window w, there is a gateway $g \in G$ towards the data center's active server (Ω). All receiving data from various patients to active servers in cloud data centers via a gateway is represented by the equation in Eq. 3.

$$\sum_{i=1}^{p} H_{i,g}(w) = \sum_{j=1}^{g} H_{j,\Omega}(w) = \sum_{\ell=1}^{\Omega} \sigma_{\ell}(w) \tag{3}$$

The data is divided into two categories based on processing time and priority. Healthcare data, such as physician inquiries and quick analysis, may require speedy processing. Other data, such as backup, transfer, and synchronization, may take longer to complete. Priority data is similarly defined as questions that arise in emergencies, such as during surgery.

Let, $\wp_s^d(w)$ and $\wp_\Lambda^d(w)$ be short and delay processing type of of data during window w in doctor $d \in D$. Similarly $\wp_{pr}^d(w)$ and $\wp_{po}^d(w)$ be number of accessible prioritised and posteriority data during window w for processing of doctor $d \in D$, where $\wp_s^d = \wp_{pr}^d + \wp_{po}^d$. The incoming rate of $H(w)$ is constrained by data $\wp(w)$ during each window w is represented in Eq. 4 and Eq. 5.

$$\begin{aligned} \wp_s^d(w) + \wp_\Lambda^d(w) &= \sum_{i=1}^{p} H_{i,g}(w) \\ &= \sum_{j=1}^{g} H_{j,\Omega}(w) = \sum_{\ell=1}^{\Omega} \sigma_{\ell}(w) \end{aligned} \tag{4}$$

$$\begin{aligned} \wp_\Lambda^d(w) + \wp_{pr}^d + \wp_{po}^d &= \sum_{i=1}^{p} H_{i,g}(w) \\ &= \sum_{j=1}^{g} H_{j,\Omega}(w) = \sum_{\ell=1}^{\Omega} \sigma_{\ell}(w) \end{aligned} \tag{5}$$

D. PRMS SYSTEM ARCHITECTURE

Figure 3 proposed PRMS system architecture is designed and focuses entirely on the security of patient health records, which will be stored in a third-party cloud database. The following steps illustrate how the entire architecture will function to secure patient health records and appropriately grant doctors access rights.

1) Every user (Doctor/Patient/Relative) must register with the system and provide reliable information.
2) The user management module validates user information. User registration information is sent to the cryptography module, which encrypts all data using the AES-128 algorithm and stores it in images using the steganography LSB technique.
3) Suppose a registered user, such as a patient, wants to store sensitive data on the cloud. In that case, the patient will send all of the data after logging in to the PRMS system and using the steganography module, which will hide all of the patient's EHRs in a single image after encrypting data with the AES-128 algorithm and provide security to the patient's EHR in a third-party cloud.
4) The patient will grant doctor/user access to their EHR data through the access control module. A patient will define some sensitive EHR that no one else in the system will see, which the anonymization module will protect.
5) If a registered doctor/user wants to access a patient's EHR, they must first login with their credentials in PRMS cloud-based e-health application and then request the patient's EHR through the access control module.
6) The access control module will verify the doctor/relative/access user's rights/privileges and contact the stegano module (steganography) to provide the requested EHR of the patient, stored in an Image in an encrypted format.
7) The steganography module will reverse the process and provide the patient's EHR to the access control module. The access control module will validate the EHR with the anonymization module.
8) The anonymization module will hide defined sensitive EHR of patients that cannot be disclosed to anyone, while the rest of the EHR will be given to the access control module.
9) Finally, the access control module will provide the patient's requested EHRs(E-Healthcare Records) to the doctor/user.

The proposed system can be defined as a five-step data security approach.

1) Authentication and authorization
2) Steganography to hide patient's EHR in Image after AES-128 encryption
3) Access control mechanism
4) Data hiding mechanism
5) Hybrid technique for combining AES-128 with steganography

An additional layer of data protection, authenticity, and cloud accessibility is proposed with the five-step process. The above steps are elaborated below in detail.

1) AUTHENTICATION AND AUTHORIZATION USING CRYPTOGRAPHIC ENCRYPTION

Cryptography encryption techniques can be used for safeguarding patient credentials in the cloud. New methods of promoting health and lowering healthcare costs even though data can be kept encrypted in servers, the user has no control over whom the data is shared. This is technically related to the issue of who owns the data encryption keys required to decrypt the data. Currently, cloud service providers, not users, have complete access to the key. In practice, users no longer have full control over their data. Giving patients control over their data, typically stored in cloud-based services, can increase trust and adoption of these applications [43]. We significantly contribute to a secure PRMS cloud-based system that allows patients to share their data with doctors and others while retaining full ownership. Encryption is critical

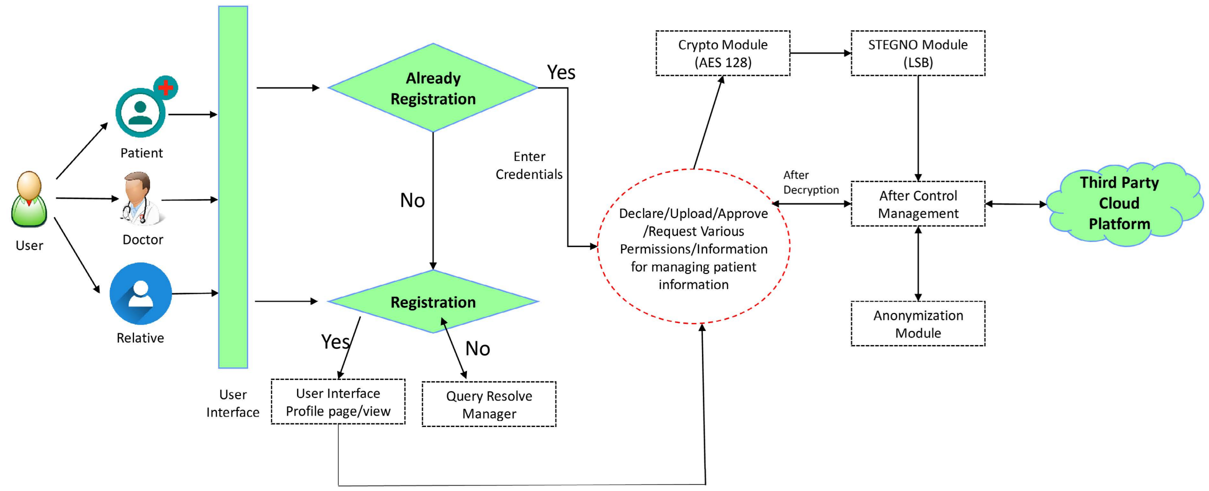


FIGURE 3. PRMS system architecture.

in healthcare IT security, but not everyone understands how it works. Users have many options when it comes to making data unreadable. AES, Blowfish, RSA (Rivest, Shamir, Adleman), and 3DES (Triple Data Encryption Standard) are examples of encryption algorithms. Solid functions, truncation, index tokens, and pads are used in one-way hashing. Encryption of high quality is essential, but it is only the initial step in safeguarding your data. Specific data security and privacy protection challenges in a cloud computing environment are outlined, along with a method for providing various security services, including authentication, authorization, and encryption, in a cloud computing environment. Advanced Encryption Standard (AES) encryption with a 128-bit key length is often used to strengthen data security and privacy [15].

2) STEGANOGRAPHY TO HIDE PATIENT's EHR IN IMAGE AFTER AES-128 ENCRYPTION

The art of hiding data within other data is known as steganography. The LSB approach can hide secret information such as messages, photos, audio, and video within the cover image. Each bit of text or image is replaced with the least significant bit of the original image using the least significant bit technique [44]. Our idea is to use the LSB method and the AES -128 algorithm to secure the secret information contained within the cover picture for patient EHRs (E-Healthcare Records) stored on a third-party cloud.

3) ACCESS CONTROL MECHANISM IN PRMS

The patient uses the access control mechanism to assign privileges and rights for the patient's EHR to doctors/users. Any healthcare institution should be able to access a patient's electronic health record, ensuring that perhaps a patient can be seen at any time. To assure data availability, health care institutions depend on internet-accessible data repositories. This creates risk because unauthorized personnel can access patient data [45]. Our system access control module is designed where various roles and privileges have been set up. In addition to, the medical staff, relatives, doctors, and patients, must be granted access to these access control systems. The access control module is designed in such a way that only part of the data report is to be given by a patient to a doctor as per their request. Whole patient data will not be available to the doctor. The system's identified users are separated into three categories: 1) Patient: A patient has all control over their medical record over the cloud. A patient can set up rights and give access rights to different users who can see patient's data over the cloud platform. Users who can only access and set privileges to their individual information are referred to as patients. 2) Doctor: All doctors, nurses, and therapists are included. They can only view clinical data from their assigned patients. They can consult online with the assigned patient. They can request specific data from a patient and schedule live consultations. 3) Relative: The person to whom a patient will grant access to their medical records in the event of an emergency.

4) DATA HIDING MECHANISM

e-healthcare allows for complete patient privacy while making efficient use of Information and Communication Technology (ICT) because patients have the right to approve or refuse anyone access to their records. Patients will be able to control who has what access to their EHR with patient-centric access control. This not only meets privacy requirements, but it also enables the e-healthcare system to earn patient trust, a vital component for e-healthcare system success [46]. Anonymization is employed in the proposed PRMS approach. Physicians can have level access, which will allow them to observe both the patient's medical status and reports, diagnoses, and treatments. The proposed PMRS e-healthcare system will be more secure and efficient with this segregated approach. Anonymization will let patient privatize their records from showing in any user in the cloud other than the patient. A patient can change their record access from specific doctor public to private.

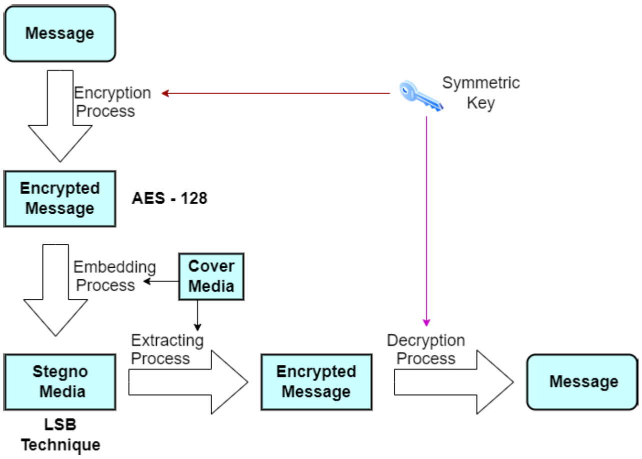


FIGURE 4. Securing data using steganography and encryption.

5) HYBRID TECHNIQUE FOR COMBINING AES-128 WITH STEGANOGRAPHY

The proposed technique integrates the Least Significant Bit (LSB) matching steganography algorithm. To ensure two-layer security of the e-health records in the third-party cloud database, the Advanced Encryption Standard (AES) technique is used before applying the steganography technique. As shown in Figure 4 how encryption, and steganography are used to secure data before being stored in a third-party cloud database.

1) Select a cover image.
2) If text, enter it into the system.
3) Use AES-128 algorithm to encrypt the text for encryption.
4) Include the encrypted data in the cover proposed image using the LSB technique.
5) The system saves the stegano image.
6) Store stegano Image in third-party cloud database.

Our plan is to safeguard the cover image's secret information using the AES method and the LSB approach. To begin, examine the image on the cover and take note of any hidden information. The next step is to use AES-128 to encrypt the data. To keep the data safe from attackers, the result of the encryption is hidden in the cover image. This is done with the help of an LSB encoder, which scrambles each pixel and stores the result in a cloud database. The components of LSB substitution for steganography are as follows: 1. LSB Encoder 2. LSB Decoder

LSB encoder function is used to disguise each encrypted text bit within the least significant bit of each 8-pixel value that forms the cover image for an encrypted message. In order to obtain the stegano-image, the output that was produced is first converted back to pixel values. Insert the stegano image to retrieve the original message from the stegano-image. LSB decoder separates the cover image and the secret encrypted message. After that symmetric key is used to get back the original message from the encrypted message.

E. PRMS SYSTEM FLOW

To ensure the confidentiality of medical data, we used a combination of cryptography and steganography in proposed Algorithm 1. Both AES cryptography and LSB steganography were used in proposed PRMS approach. Encrypting and decrypting sensitive health care data using the Advanced Encryption Standard (AES) is the industry standard. The Advanced Encryption Standard (AES) is a symmetric block cipher that supports a block size of up to 128 bits. The number of rounds in the encryption process is based on the length of the key, the number of rounds for AES-128 is 10. The following operations are carried out by the primary loop of the AES:

- SubBytes()
- ShiftRows()
- MixColumns()
- AddRoundKey()

To begin the AES encryption process, the 16-byte input array is copied into a 4 × 4 byte matrix called state. The input data block, state, is XORed with the first 128 bits of the cipher key. The resulting state is then transmitted through ten consecutive cycles. The previous round's outcome was encrypted data. The EHR data is symmetrically encrypted using the AES algorithm key. In order to hide the encrypted data, steganography is used for double layer protection. Patient's personal information such as their name, age, and patient EHR are entered into the system as input. The AES algorithm with 128-bit secret key used to encrypt the input data. The LSB technique is used to conceal encrypted data within a cover stegano image. The image is then sent to a third-party cloud database for storage. The data is first extracted from the stegano image by the receiver using the LSB technique and then decrypted using the AES algorithm with the same secret key of 128 bits. After that, the original data can be retrieved. The proposed Algorithm 1 combines AES-128 with LSB steganography techniques to store e-health records in a third-party cloud environment as follows:

IV. PRMS SYSTEM DESIGN IMPLEMENTATION

This section represents a system implemented in third-party cloud AWS (Amazon Web Service) and GCP (Google Cloud Platform). A Complete system for handling the EHR of the patient over the cloud. Some of the PRMS system design is shown below in figure 5, 6, 7, 8, 9, 10. Patients, doctors, and other family members use their unique ID and password to access the system. Users have to enter valid information for registration to use the PRMS e-health cloud-based web application. A patient/doctor/relative will be registered with their details. Registration detail is encrypted using AES-128 and stored in Image using the steganography LSB technique in the database. A unique ID will be generated for further login. As per role, the system will display a unique dashboard for user features. If the user's role is patient, after successful login, the patient is redirected to its dashboard, and the patient can access different system features from its dashboard. A patient dashboard will have facilities for a live

Algorithm 1 Combining AES – 128 Algorithm With Steganography

```
Input: E-Health Records (EHR), Cipher Key K.
Output: Cipher Health Record (CHR) stored in
        image over third-party cloud database
1  Create a key expansion of K that generates two lists
   of all sub keys.
2  Consider Partition EHR into 16-byte blocks ($B_1$, $B_2$,
   $B_3$,...$B_n$).
3  for $B_i$ block do
4      Divide $B_i$ into two arrays of $4 \times 4$ size
5      Perform Nine rounds manipulation following
       steps shown from Step 6 to Step 9
6      Substitute bytes using predetermined e-healthcare
       table.
7      Shift rows.
8      Mix columns.
9      Add round keys.
10     Array out the tenth and final round of state
       manipulation.
11     Consider a copy of the final State array as the
       encrypted information (ciphertext) CHR.
12     Convert the CHR from binary to decimal.
13     Select cover image C1.
14     Apply LSB encoder to C1.
15     Calculate LSB of each pixels of cover image.
16     Replace LSB of cover image with each bit of
       secret message one by one.
17     Write stegano image.
18     Return the stegno-ciphered image.
19     Store stegano image in third party cloud database.
20 end
```

consultation with a doctor, uploading various reports, doctor access requests for EHR, and inserting medical records in the cloud. The system ensures double-layer protection for the patient's EHR in a third-party cloud database. Patient medical data will be stored privately in a third-party cloud database, and permission is required to access it from the patient. All patient reports will be kept private in the database. A patient can assign access rights to different EHR reports to a specific doctor. A patient can give access rights for EHR to their relatives during emergencies if required through the registration process in PRMS. If the user role is doctor, the doctor is redirected to its dashboard. A doctor can access various features given in the system. A doctor can search for a patient in the system by its patient ID. The doctor dashboard will have an appointment, search patient records, and request patient reports and medical data from the patient. The doctor can request patient text data and medical report access rights from its dashboard. Patients can approve text medical records and patient medical reports requested by the doctor from the patient's dashboard. A patient can send a request from their dashboard to schedule an appointment with a specific doctor.

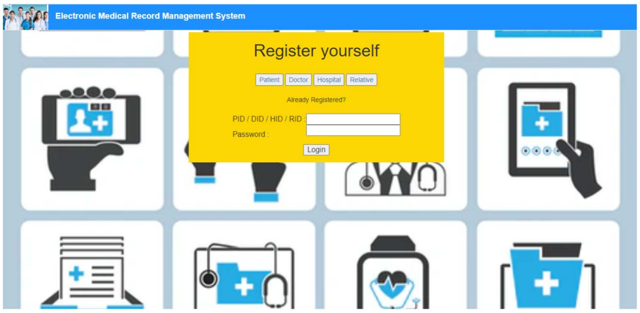
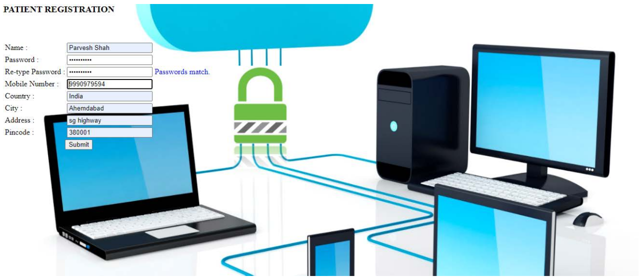
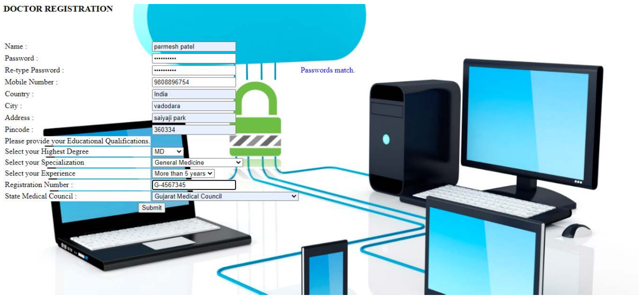


FIGURE 5. Home page.


PATIENT REGISTRATION

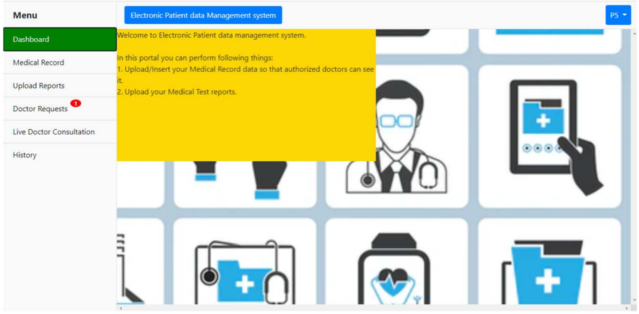
Name : Parvesh Shah
Password : ••••••••••
Re-type Password : •••••••••• Passwords match.
Mobile Number : 9990979594
Country : India
City : Ahemdabad
Address : sg highway
Pincode : 380001

FIGURE 6. Patient registration screen.


DOCTOR REGISTRATION

Name : parmesh patel
Password : ••••••••••
Re-type Password : •••••••••• Passwords match.
Mobile Number : 9808896754
Country : India
City : vadodara
Address : saiyaji park
Pincode : 360334
Please provide your Educational Qualifications.
Select your Highest Degree MD
Select your Specialization General Medicine
Select your Experience More than 5 years
Registration Number : G-4567345
State Medical Council : Gujarat Medical Council

FIGURE 7. Doctor registration screen.



Welcome to Electronic Patient data management system.

In this portal you can perform following things:
1. Upload/Insert your Medical Record data so that authorized doctors can see it.
2. Upload your Medical Test reports.

FIGURE 8. Patient dashboard.

A patient can schedule an appointment or see a doctor at any available time. Doctors can view appointment schedules for a particular patient for interaction.

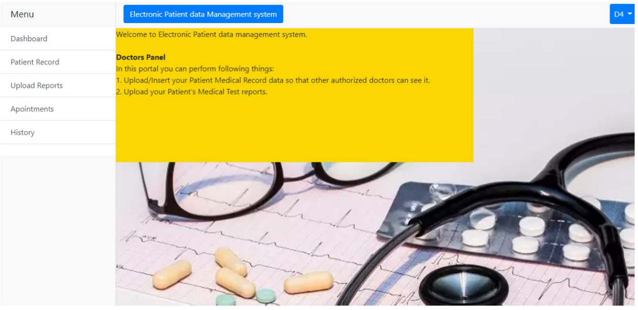
V. EXPERIMENTAL SETUP

A. EXPERIMENT 1: COMPARING CLOUD BASED CUSTOMIZED THIRD PARTY PLATFORMS WITH BLOCKCHAIN PLATFORMS

This experiment focuses solely on comparing the performance of cloud-based customized encryption AES-128

TABLE 2. System configuration.

Parameter	GCP	AWS	Etherium 1.5.8	Hyperledger 0.6
RAM	2 GB	1GB	64GB	64GB
OS	Linux	Amazon Linux	Ubuntu16.04	Ubuntu16.04
Virtual CPU	1	1	8	8
Engine	App Engine	EC2	EC2	EC2
Apache2	2.4.38	2.4.52	2.4.3.8	2.4.3.8
MySQL Client-Server	5.7.36	7.4.27	—-	—-
PHP version	7.4.25	7.4.27	7.4.25	7.4.25
Instance	LAMP-1-vm	t2micro	c4.2xlarge	c4.2xlarge



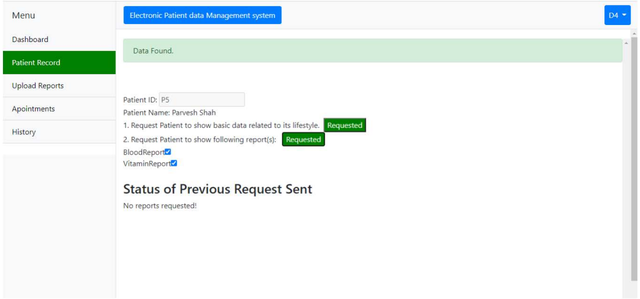
Welcome to Electronic Patient data management system.

Doctors Panel

In this portal you can perform following things:

1. Upload/Insert your Patient Medical Record data so that other authorized doctors can see it.
2. Upload your Patient's Medical Test reports.

FIGURE 9. Doctor dashboard.



Data Found.

Patient ID: P5

Patient Name: Parvesh Shah

1. Request Patient to show basic data related to its lifestyle. Requested
2. Request Patient to show following report(s): Requested

BloodReport ☑

VitaminReport ☑

Status of Previous Request Sent

No reports requested!

FIGURE 10. Doctor dashboard request.

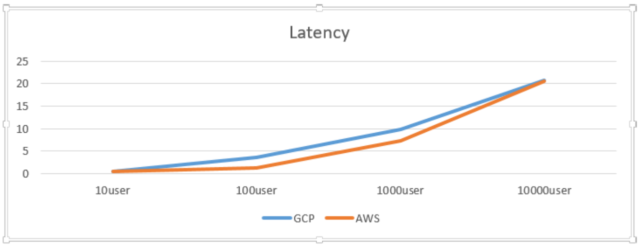


FIGURE 11. Patient registration latency.

algorithm using steganography with Blockchain. Hyperledger Fabric and Ethereum are tested in terms of throughput and latency with up to 10,100,1000,10000 user transactions using AWS and GCP third-party cloud providers with e-health care records integrated with encryption, steganography, and access control rights to the user in order to assess their current status. To evaluate the platform's throughput and latency, paper [47] creates a synthetic application for the experiments that functions as a cash transfer application and allows a user account to be created (via the function Create account) in Hyperledger and Ethereum platforms. We have compared the work of [47] for creating an account function with our application in a cloud environment that inserts records from patients. To evaluate our cloud encryption system with Ethereum and Hyperledger, we hosted our system in third-party cloud providers AWS (Amazon Web Service) and GCP (Google Cloud Platform). For comparing the cloud-based health system, insert and select e-health records of a patient, the experiments are conducted on the GCP and AWS. HTTP requests in the Node.js application are used to communicate between the client and the Blockchain platform in the communication. JSON RPC API calls are used to interact between web3.js and a local node for Ethereum inquiries. In Hyperledger Fabric, RESTful APIs are used to implement all queries [47]. JMeter tools are used in two experiments for cloud customized encryption using steganography to protect patient's e-health records hosted on third-party cloud providers AWS and GCP. Then we looked at [47]'s Hyperledger fabric 0.6 and Ethereum 1.5.8 performance. For the performance evolution of two different cloud and Blockchain technologies, we assessed latency and throughput by different loads, such as the number of queries fired by the user on the GCP service and AWS. The transaction is measured from the time the transaction is submitted to the peers for consensus to the time the transaction is added to a block. System configuration for comparing Blockchain platforms and third-party cloud platform system configuration is shown in Table 2.

B. EXPERIMENT 1: RESULTS AND DISCUSSION

Here in Results and Discussion of Experiment 1, we test and compare the performance of the Blockchain platform and e-health application hosted on third-party cloud platform AWS and GCP with encryption and steganography in the context of latency and throughput. Firstly, as per implemented system architecture for the security experiment result of patient registration and doctor registration measured by JMeter. JMeter results of latency and throughput of GCP and AWS is shown. For Blockchain technology, performance analysis of Ethereum vs. Hyperledger is used as described in the paper [47].

Based on the Jmeter result, we can deduce that GCP has the edge over the AWS service with our custom encryption steganography system architecture. Here Figure 11 and

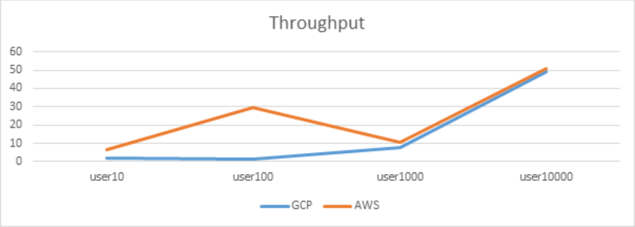


FIGURE 12. Patient registration throughput.

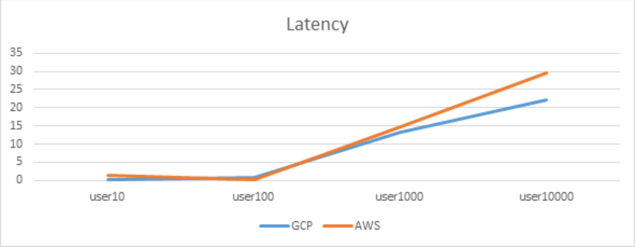


FIGURE 13. Doctor registration latency.

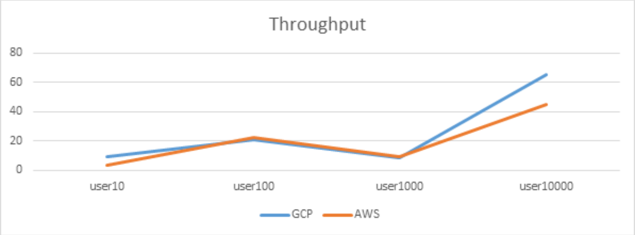
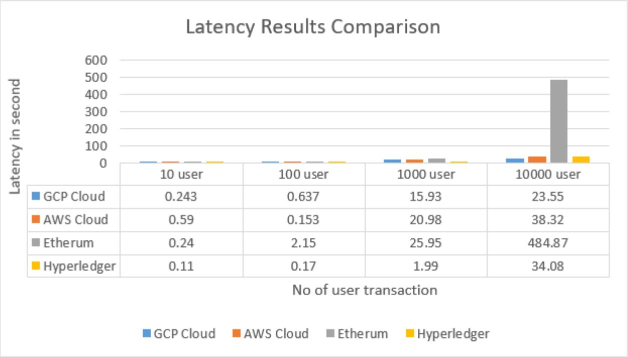


FIGURE 14. Doctor registration throughput.



	10 user	100 user	1000 user	10000 user
GCP Cloud	0.243	0.637	15.93	23.55
AWS Cloud	0.59	0.153	20.98	38.32
Etherum	0.24	2.15	25.95	484.87
Hyperledger	0.11	0.17	1.99	34.08

FIGURE 15. Cloud platform vs blockchain platform latency comparison.

Figure 12 show the patient registration latency and throughput result, and Figure 13, Figure 14 offers the doctor registration latency and throughput, which give GCP an edge by reducing the latency over AWS.

In Figure 15 and Figure 16, we discovered a difference in latency when a different number of transactions were checked with various platforms such as Google Cloud Platform (GCP), Amazon Web Service (AWS), Ethereum Blockchain, and Hyperledger Blockchain. Latency increases with the increase in the number of transactions. The latency value of a cloud-based platform is consistently lower than

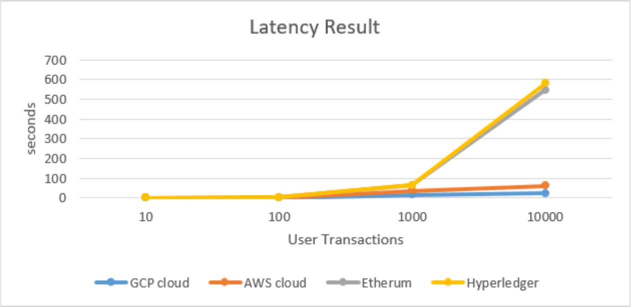


FIGURE 16. Cloud platform vs Blockchain platform Latency Line chart comparison.

the latency value of a Blockchain platform. When a very large number of transactions were used, the latency went up a little bit in the Blockchain platform. When transactions have fewer operations, they can support a very high number, like 100,000, with a very low latency. It also depends on the hardware chosen and the way the Blockchain network is set up. When the number of simultaneous transactions goes up, it has a big overall impact on how well the Blockchain network works, especially the latency. Traditional Blockchains have been affected by the issue of scalability. As a result, maintaining multiple copies of e-healthcare data and ensuring consistency is a burden that comes with decentralization. In addition, Blockchain require a lot of computing power and a lot of energy.The idea of using Blockchain to store data in a decentralized manner is often widely regarded. Blockchain storage, on the other hand, comes at a price. Analysis estimated that one megabyte of data on the Ethereum network would cost in U.S dollars, whereas Amazon Simple Storage Service would only charge a few cents (S3). Cloud services trust, security policies and governance layers are sufficiently accurate for most enterprise applications. In addition, there are numerous third-party data storage services that can provide better governance and security for a relatively lower price than a Blockchain.The overall decision to use Blockchain technology in healthcare is heavily influenced by the costs involved.

In Figure 17 & Figure 18 we discovered a difference in throughput when a different number of transactions were checked with various platforms such as Google Cloud Platform, Amazon Web Service, Ethereum Blockchain, and Hyperledger Blockchain. Throughput increases with the increase in the number of transactions. The performance of a network is directly impacted by the latency and throughput it experiences. Packets will take longer to reach their destination if latency is too high. When packets take longer to reach their final destination, network services and applications will be slower to respond to requests. The lower the throughput, the fewer packets can be processed in a given amount of time. Because the PRMS approach uses encryption and steganography to store data over a third-party cloud, it's critical to optimize to reduce causes of latency and to test PRMS hosted on different third-party clouds to manage patient's e-healthcare records performance. The performance evaluation of the two platforms will be assessed in terms of latency, and throughput, by varying the workload in each platform up to 10,000 transactions. With 10 user transactions, the average latency of Hyperledger and Ethereum is 0.11 seconds and 0.24 seconds, respectively, as in our cloud-based PRMS e-health application, which is 0.24 seconds for GCP and 0.59 seconds for AWS. Hyperledger's average latency is 34.08 seconds, while Ethereum's is 484.87 seconds, and both are steadily increasing when the number of transactions reaches 10,000. When we compare with our cloud-based PRMS e-health application hosted on GCP and AWS, the average latency for GCP is 23.55 seconds and the average latency for AWS is 38.32 seconds. Let us look at the average throughput of Hyperledger and Ethereum with 10 user transactions. It is 68.02 seconds and 27.49 seconds, respectively, as in our cloud-based PRMS e-health application, 8.6 seconds for GCP, and 6.6 seconds for AWS. When the number of transactions reaches 10,000, the average throughput of Hyperledger is 159.76 seconds, and that of Ethereum is 29.6 seconds. The average throughput for our cloud-based PRMS e-health application hosted on GCP and AWS is 10.7 seconds and 10.5 seconds, respectively. As it can be seen from the charts, cloud-based steganographic encryption has comparable throughput and lower latency than Ethereum. However, in the case of Hyperledger, its performance is comparable to cloud encryption when the workload is varied up to 10,000 transactions. It can be observed that even though lower system configuration compared to Blockchain platforms, cloud encryption with steganography performs better than Ethereum and Hyperledger in all metrics. Based on the above experiment result, we can make a statement that the cloud with encryption logic gives the lowest latency compared to the Blockchain platform. The cost of a cloud-based platform is consistently lower than a Blockchain platform. As this study is in its early stages, it has several limitations. Research into the use of third-party cloud in healthcare is still in its infancy, but we expect to contribute to the adoption of an open-source framework for auditing and monitoring electronic health data. We are looking into using NoSQL-based databases to dynamically scale out the database tier instead of statically allocating over-provisioned resources for PRMS in the third-party cloud deployment. It can help lower operational costs.

C. EXPERIMENT 2: COMPARISON OF PRMS WITH SRHB APPROACH FOR SECURE TRANSMISSION OF HEALTHCARE DATA

The proposed PRMS method employs customized stenographic encryption to transmit healthcare information securely deployed on AWS and the GCP platform. To evaluate the performance of the proposed mechanism, which expresses the average delay and system execution, we have compared the proposed PRMS with paper [48] containing the average delay and system execution time of the Secure and Robust Healthcare-based Blockchain (SRHB) approach. The average delay is the difference between when the medical records were sent and when they were received at the moment. It shows a medical delay between the patient and the doctor or relative and the other way around.The estimated System Execution Time (SET) includes both the total number of medical records as well as the average retrieval time for those records. The Secure and Robust Healthcare-based Blockchain (SRHB) solution, which leverages Attribute-based Encryption to securely transport healthcare data, is described in this study [48]. The SRBH deployment was carried out using a laptop running Windows 8 64-bit and an Intel i3 Core CPU. The application was developed using NetBeans 8.2, JDK 1.8, Apache Tomcat 8.0.15, MYSQL 5.7, and the Jelastic cloud environment. AWS and Google Cloud Platform (GCP) have been used for the implementation of PRMS. Google App Engine (LAMP VM -1 instance) with 1 core vCPU, 2 GB RAM, and Linux OS is used for the experiments on GCP. EC2 (t2. micro instance) with 1 core vCPU and 1 GB RAM is used for the experiments on AWS, which uses Amazon Linux OS. The proposed PRMS approach and SRHB approach both were analyzed for Yahoo Cloud Serving Benchmark (YCSB) and the small bank dataset. Comparison of the system configuration of AWS, GCP for PRMS, and Jelastic cloud environment used in SRHB approach is shown in Table 3.

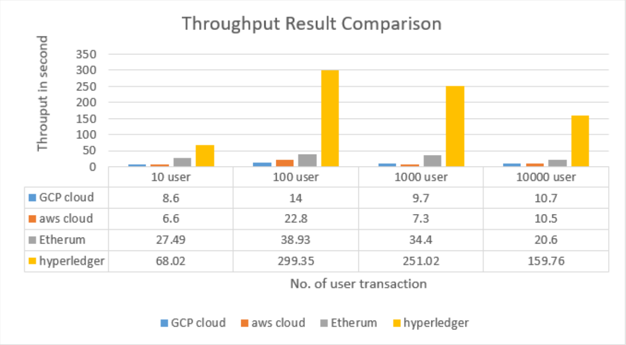


FIGURE 17. **Cloud platform vs blockchain platform throughput comparison.**

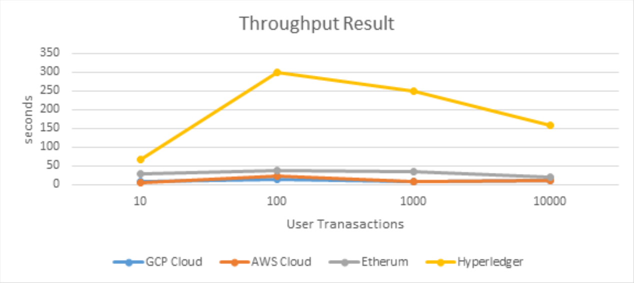


FIGURE 18. **Throughput line chart cloud platform vs Blockchain.**

D. EXPERIMENT 2: RESULTS AND DISCUSSION

The process of sharing medical records and retrieving medical records from the storage web server takes the SRHB approach [48] significantly takes more time. The PRMS approach that has been proposed is reliable with a cloud storage server, and it can work on its own to facilitate

TABLE 3. System configuration.

Parameter	AWS	GCP	Jelestic cloud
Approach	PRMS	PRMS	SRHB
RAM	1 GB	2 GB	8 GB
OS	AMAZON Linux	Linux	Windows 8
Virtual CPU	1	1	i3
Apache2	2.4.38	2.4.52	8.0.15

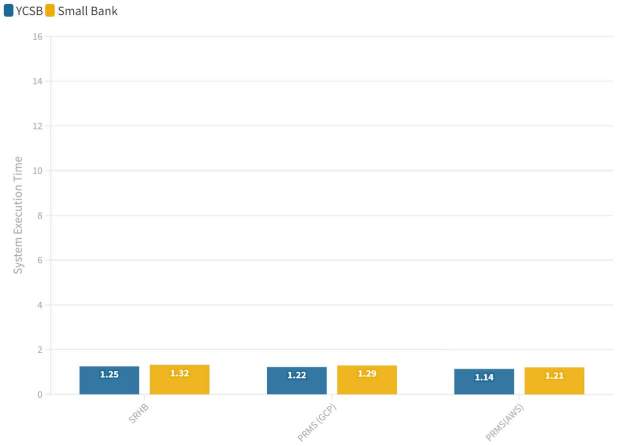


FIGURE 19. System execution time in seconds for YCSB and small bank dataset.

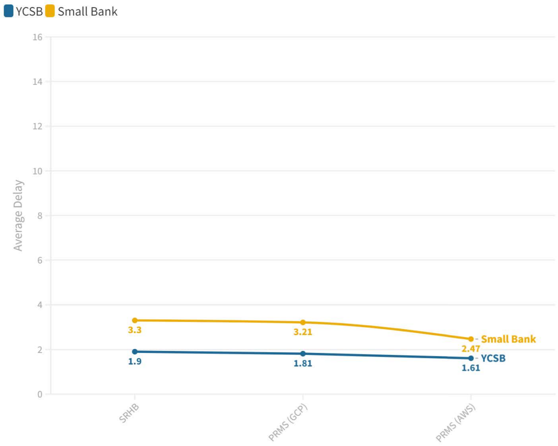


FIGURE 20. Average delay in seconds for YCSB and small bank dataset.

the secure sharing of information and the retrieval of the information from the cloud storage server. The experimental results of PRMS system execution time and average delay compared to the SRBH approach, the SRHB approach significantly slows down the process of sharing and retrieving medical records from the storage web server in comparison to PRMS approach. In AWS, the proposed PRMS reduces 1.61 AD and 2.47 AD (Average Delay) in seconds for YCSB and small bank datasets, respectively, and 1.14 SET and 1.21 SET (System Execution Time) in seconds for YCSB and small bank datasets, respectively. In Google Cloud Platform (GCP), the proposed PRMS reduces 1.81 AD and 3.21 (Average Delay) in seconds for YCSB and small bank datasets, and 1.22 SET and 1.29 SET (System Execution Time) in seconds for YCSB and Small Bank datasets, respectively. The proposed PRMS approach average delay and system execution time are analyzed with the SRHB approach for YCSB, and small bank datasets are shown in Figure 19 and Figure 20.

VI. CONCLUSION

This paper examines the effectiveness of steganography encryption in a cloud environment by comparing latency and throughput with Ethereum and Hyperledger fabric platforms with varying transaction numbers. It is a significant challenge to ensure the security of patient's e-health records in the cloud. Additionally, the proposed PRMS (Patient Medical Records Management System) is compared to the Secure and Robust Healthcare-based Blockchain method (SRHB) in terms of System Execution Time (SET) and Average Delay. The efficiency of the proposed PRMS architecture has many quality matrices like maintaining user privacy, effective medical data sharing, and information hiding. PRMS is a security architecture that uses cryptography and steganography to protect patient health records in the third-party cloud from unauthorized access while also allowing patients to control their health records. The entire system was constructed, and some of the system design of the PRMS cloud-based e-health application was described in the paper. Each architecture developed has room for improvement. Other hiding and cryptographic techniques can be added to the PRMS in the future for better results.

A. FUTURE WORK

Future work will include the addition of data encryption and cloud storage security algorithms to the PRMS system in order to further enhance the cloud security of patient data. External access to e-healthcare data transferred across multiple networks will be the subject of additional data security and privacy analyses in the near future.

REFERENCES

[1] M. Azhagiri, R. Amrita, R. Aparna, and B. Jashmitha, "Secured electronic health record management system," in *Proc. 3rd Int. Conf. Commun. Electron. Syst. (ICCES)*, Oct. 2018, pp. 915–919.

[2] N. Dong, H. Jonker, and J. Pang, "Challenges in ehealth: From enabling to enforcing privacy," in *Proc. Int. Symp. Found. Health Informat. Eng. Syst.* Cham, Switzerland: Springer, 2011, pp. 195–206.

[3] X. Yi, Y. Miao, E. Bertino, and J. Willemson, "Multiparty privacy protection for electronic health records," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 2730–2735.

[4] C. S. Kruse, M. Mileski, A. G. Vijaykumar, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram, "Impact of electronic health records on long-term care facilities: Systematic review," *JMIR Med. Informat.*, vol. 5, no. 3, p. e35, Sep. 2017.

[5] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "EHealth cloud security challenges: A survey," *J. Healthcare Eng.*, vol. 2019, pp. 1–15, Sep. 2019.

[6] H. K. Thakkar, C. K. Dehury, and P. K. Sahoo, "MUVINE: Multi-stage virtual network embedding in cloud data centers using reinforcement learning-based predictions," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1058–1074, Jun. 2020.

[7] H. K. Thakkar, P. K. Sahoo, and B. Veeravalli, "RENDA: Resource and network aware data placement algorithm for periodic workloads in cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 12, pp. 2906–2920, Dec. 2021.

[8] J. Zaki, S. M. R. Islam, N. S. Alghamdi, M. Abdullah-Al-Wadud, and K.-S. Kwak, "Introducing cloud-assisted micro-service-based software development framework for healthcare systems," *IEEE Access*, vol. 10, pp. 33332–33348, 2022.

[9] S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar, and R. A. Khan, "A systematic analysis on blockchain integration with healthcare domain: Scope and challenges," *IEEE Access*, vol. 9, pp. 84666–84687, 2021.

[10] S. U. Amin and M. S. Hossain, "Edge intelligence and Internet of Things in healthcare: A survey," *IEEE Access*, vol. 9, pp. 45–59, 2021.

[11] S. Ali, S. Khusro, and A. Rauf, "A cryptography-based approach to web mashup security," in *Proc. Int. Conf. Comput. Netw. Inf. Technol.*, Jul. 2011, pp. 53–57.

[12] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health cloud: Opportunities and challenges," *Future Internet*, vol. 4, no. 3, pp. 621–645, 2012.

[13] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," *Int. J. Inf. Manage.*, vol. 43, pp. 146–158, Dec. 2018.

[14] S. Camarasu-Pop, F. Cervenansky, Y. Cardenas, J.-Y. Nief, and H. Benoit-Cattin, "Overview of medical data management solutions for research communities," in *Proc. 10th IEEE/ACM Int. Conf. Cluster, Cloud Grid Comput.*, May 2010, pp. 739–744.

[15] M. Babitha and K. R. Babu, "Secure cloud storage using AES encryption," in *Proc. Int. Conf. Autom. Control Dyn. Optim. Techn. (ICACDOT)*, Sep. 2016, pp. 859–864.

[16] M. Sajjad, K. Muhammad, S. W. Baik, S. Rho, Z. Jan, S.-S. Yeo, and I. Mehmood, "Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3519–3536, 2017.

[17] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Mar. 2017.

[18] E. Yuan and J. Tong, "Attributed based access control (ABAC) for web services," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jul. 2005, pp. 561–569.

[19] D. Mashima and M. Ahamad, "Enhancing accountability of electronic health record usage via patient-centric monitoring," in *Proc. 2nd ACM SIGHIT Symp. Int. Health Informat. (IHI)*, 2012, pp. 409–418.

[20] X. Sun, M. Li, H. Wang, and A. Plank, "An efficient hash-based algorithm for minimal k-anonymity," in *Proc. 31st Australas. Conf. Comput. Sci.*, vol. 74, Jan. 2008, pp. 101–107.

[21] E. Kamalakannan and K. S. Arvind, "Privacy conserving and secure distribution of personal health information using cloud," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2014, pp. 1–4.

[22] P. Tasatanattakool and C. Techapanupreeda, "User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Dec. 2017, pp. 1019–1024.

[23] C. Xu, J. Wang, L. Zhu, C. Zhang, and K. Sharif, "PPMR: A privacy-preserving online medical service recommendation scheme in eHealthcare system," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5665–5673, Jun. 2019.

[24] W. Liu, X. Liu, J. Liu, Q. Wu, J. Zhang, and Y. Li, "Auditing and revocation enabled role-based access control over outsourced private EHRs," in *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun. 7th Int. Symp. Cyberspace Saf. Secur., IEEE 12th Int. Conf. Embedded Softw. Syst.*, Aug. 2015, pp. 336–341.

[25] M. Zhang and Y. Ji, "Blockchain for healthcare records: A data perspective," *PeerJ Preprints*, vol. 6, May 2018, Art. no. e26942v1.

[26] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, vol. 13, Apr. 2016, p. 13.

[27] I. Radanović and R. Likić, "Opportunities for use of blockchain technology in medicine," *Appl. Health Economics Health Policy*, vol. 16, no. 5, pp. 583–590, Jul. 2018.

[28] M. Bartoletti, S. Lande, L. Pompianu, and A. Bracciali, "A general framework for blockchain analytics," in *Proc. 1st Workshop Scalable Resilient Infrastruct. Distrib. Ledgers*, Dec. 2017, pp. 1–6.

[29] B. Koteska, E. Karafiloski, and A. Mishev, "Blockchain implementation quality challenges: A literature," in *Proc. SQAMIA 6th Workshop Softw. Qual., Anal., Monitor, Improvement, Appl.*, vol. 11, 2017, p. 8.

[30] R. Yasaweerasinghelage, M. Staples, and I. Weber, "Predicting latency of blockchain-based systems using architectural modelling and simulation," in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Apr. 2017, pp. 253–256.

[31] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *Int. J. Med. Informat.*, vol. 142, Oct. 2020, Art. no. 104246.

[32] P. Genestier, S. Zouarhi, P. Limeux, D. Excoffier, A. Prola, S. Sandon, and J.-M. Temerson, "Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges," *J. Int. Soc. Telemed. eHealth*, vol. 5, Apr. 2017, Art. no. GKR-e24.

[33] A. Clim, R. D. Zota, and R. Constantinescu, "Data exchanges based on blockchain in m-health applications," *Proc. Comput. Sci.*, vol. 160, pp. 281–288, Jan. 2019.

[34] K. Shuaib, H. Saleous, K. Shuaib, and N. Zaki, "Blockchains for secure digitized medicine," *J. Personalized Med.*, vol. 9, no. 3, p. 35, Jul. 2019.

[35] B. B. Gupta, K.-C. Li, V. C. M. Leung, K. E. Psannis, and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 12, pp. 1877–1890, Dec. 2021.

[36] V. A. Memos, K. E. Psannis, S. K. Goudos, and S. Kyriazakos, "An enhanced and secure cloud infrastructure for e-health data transmission," *Wireless Pers. Commun.*, vol. 117, no. 1, pp. 109–127, Mar. 2021.

[37] C. Stergiou and K. E. Psannis, "Efficient and secure BIG data delivery in cloud computing," *Multimedia Tools Appl.*, vol. 76, no. 21, pp. 22803–22822, Nov. 2017.

[38] M. A. Bouras, Q. Lu, S. Dhelim, and H. Ning, "A lightweight blockchain-based IoT identity management approach," *Future Internet*, vol. 13, no. 2, p. 24, Jan. 2021.

[39] G. Capece and F. Lorenzi, "Blockchain and healthcare: Opportunities and prospects for the EHR," *Sustainability*, vol. 12, no. 22, p. 9693, Nov. 2020.

[40] W. Zhang, Y. Wu, B. Yang, S. Hu, L. Wu, and S. Dhelimd, "Overview of multi-modal brain tumor MR image segmentation," in *Healthcare*, vol. 9. Basel, Switzerland: Multidisciplinary Digital Publishing Institute, 2021, p. 1051.

[41] H. Ning, S. Dhelim, M. A. Bouras, A. Khelloufi, and A. Ullah, "Cyber-syndrome and its formation, classification, recovery and prevention," *IEEE Access*, vol. 6, pp. 35501–35511, 2018.

[42] P. K. Sahoo, S. K. Mohapatra, and S.-L. Wu, "Analyzing healthcare big data with prediction for future health condition," *IEEE Access*, vol. 4, pp. 9786–9799, 2016.

[43] D. Thilakanathan, R. A. Calvo, S. Chen, S. Nepal, and N. Glozier, "Facilitating secure sharing of personal health data in the cloud," *JMIR Med. Informat.*, vol. 4, no. 2, p. e15, May 2016.

[44] P. P. Bandekar and G. C. Suguna, "LSB based text and image steganography using AES algorithm," in *Proc. 3rd Int. Conf. Commun. Electron. Syst. (ICCES)*, Oct. 2018, pp. 782–788.

[45] D. R. Matos, M. L. Pardal, P. Adão, A. R. Silva, and M. Correia, "Securing electronic health records in the cloud," in *Proc. 1st Workshop Privacy Design Distrib. Syst.*, Apr. 2018, pp. 1–6.

[46] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2017.

[47] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–6.

[48] A. Mubarakali, "Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN(SRHB)approach," *Mobile Netw. Appl.*, vol. 25, no. 4, pp. 1330–1337, Aug. 2020.