ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

PRMS: DESIGN AND DEVELOPMENT OF PATIENTS' E-HEALTHCARE RECORDS MANAGEMENT SYSTEM FOR PRIVACY PRESERVATION IN THIRD PARTY CLOUD PLATFORMS

Javeria Sarvath
CSE Department
Shadan Women's College Of Engineering and Technology,
Hyderabad, India
sarvathjaveria98@gmail.com

Dr. K. Palani
CSE Department.
Shadan Women's College of Engineering and Technology,
Hyderabad, India
principalswcet2020@gmail.com

ABSTRACT: .

The preservation of private information on open platforms is a huge security and privacy risk in the present digital era. This is particularly true for e-health data management, where a number of defined standards must be followed while managing patient health data. Computing and storage resources are primarily offered by cloud service providers (CSPs). Data security on the cloud is still a significant issue, though. In many cases, block chain technology saves the CSPs by giving the underlying data strong security by encrypting it with special and secret keys. To protect the data, each network user has their own individual, secret key that is directly linked to the transaction keys. However, in conditions of heavy workload, technology experiences latency and throughput problems. We created a Patient's E-Healthcare Records Management System (PRMS) that prioritises latency and throughput to get around problems with e-healthcare records privacy in a third-party cloud. To verify its applicability, a thorough performance investigation of PRMS is conducted on several third-party clouds. Furthermore, by varying the workload for each platform up to 10,000 transactions per second, the proposed PRMS system is evaluated against latency and throughput for Block chain systems like Fabric v0.6 and 1.5.8. The Secure and Robust Healthcare-Based (SRHB) method and the proposed PRMS are contrasted using the Yahoo Cloud Serving Benchmark (YCSB) and a modest bank database.

2.INTRODUCTION

Data storage in cloud data centres is preferred over local systems in the current era of digital communications. Modern applications like Smart Cities, the Internet of Medical Things (IoMT), and E-Healthcare create data that is processed and stored on cloud platforms owned by Cloud Service Providers (CSPs). CSPs, however, just offer the infrastructure for data processing and storage; they do not offer a complete data security framework. CSPs frequently incorporate the third-party security architecture for data protection and privacy preservation. Third-party security frameworks, however, can have expensive integration problems. Contrarily, technology delivers immutable blocks of chain, fostering trust and transparency. When it comes to avoiding data tampering in a setting where cloud security is easily available, enabled solutions are the obvious choice. While processing several transactions, enabled security has drawbacks in terms of latency and performance. In the proposed study, we have solely concentrated on improving latency and throughput during the many transactions situations that emerge during the access to E-healthcare Records (EHRs). Even though this has proven to be a difficult process, electronic records can integrate data from numerous registered sites and provide a more complete picture of precise patient facts [1]. Despite all of the advantages the cloud has over on-premises storage, healthcare data is still at significant risk as a result. As paper-based records are gradually phased out and replaced by computerised ones, the healthcare industry is undergoing transition [2]. Digitalized electronic medical records that have replaced paper-based records include Personal Health Records (PHR), Electronic Health Records (EHR), Electronic Medical Records (EMR), and Electronic Health Data (EHD). While PHR refers to routinely storing and monitoring personal information by the patient or their family members, EHR and EMR relate to patient health records maintained by healthcare professionals. EHD is a kind of smart health record that is provided to patients [3]. It is also known as electronic health records or computerised patient records. These records include medication information, medical histories, demographic data, immunisation records, lab test results, and other private patient data. When opposed to EHD systems, traditional paper-based records have a number of limitations. EHR requires less time, labour, and physical storage than paper-based records [4]. Consumers and healthcare providers are facing a number of security and privacy challenges as a result of the centralization of data on the cloud. (1) Gives hackers a one-stop shop to exploit transmitted data and steal information, and (2) gives cloud service providers ownership rights, letting people and healthcare workers lose control of private information [5]. Users can now manage cloud data centre computing and networking resources for e-healthcare

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

data thanks to recent advances in virtualization technology [6], [7]. Patient health records are designed for patient's health care records in a cloud-assisted health care delivery system for efficiency, scalability, and performance enhancement [8]. Numerous proposed systems make use of privately held and open-source platforms, which have enormous promise for protecting patient health records and health care systems in a cloud context [9]. Due to new technology and the rapid advancements in human existence, patients nowadays require a complex and comprehensive smart healthcare framework tailored to their health requirements. The general application of IoT solutions in edge systems for medical treatment and healthcare is summarised by the authors in [10]. Additionally, the e-health system is increasingly using a cloud environment to share and manage vast volumes of distributed medical data, including EHR and lab test results. Cloud storage services provide a practical and expandable response to these enormous data management difficulties. [11], [12], [13], and [14]. Patients must have the option to provide authorised others full, partial, or selective access to their data. Consent management is what is referred to as this, and it is a crucial problem in e-Health [15]. Several techniques, such as data steganography's Least Significant Bit (LSB) method, use 8 pixels from the image to conceal one character of the secret message. The least significant bit of the associated pixel in the image is increased by each binary bit from the private message character. The least significant bit (LSB) of an image is replaced with a bit of data using the Least Significant Bit (LSB) approach of steganography (a byte has 8 bits, and the least significant bit number is 8) [16]. Steganography is the process of obscuring data with a physical object or another piece of information [16]. Technology progress makes use of fresh steganographic techniques including null cyphers, image coding, audio, and video [16]. is a technology that fundamentally alters the idea of confidence in systems of the future. It encourages carrying out any transaction without the use of a middleman. The majority of the time, centralised institutions that accept, process, and store transactions are mediators like companies and governments. All of the trust that users have in a system is placed in the intermediaries, who have a duty to handle transactions according to the right business logic. The confidentiality and privacy of the data are entirely at the mediators' control. -based systems have decentralised trust. Users merely need to have faith in the system and the universally shared smart code. Data and transactions are now saved and recorded in a whole different form as a result of. Similar to a conventional database, the goal behind is to cut out the intermediary. [17]. When the idea of a digital currency was originally put forth in 2008, that was the first time technology was used. Despite the many advantages of this technology, moving to the cloud has a number of drawbacks. The main barriers to the widespread adoption of cloud computing for the processing of medical records are security and privacy. The shared infrastructure approach as depicted in Figure 1 is entirely under the provider's control. The services for this kind of cloud system are under the jurisdiction of the Cloud Service Providers (CSPs). Electronic health records (EHRs) are frequently shared between various entities, as seen in Figure 1. EHRs are extremely vulnerable to assaults and manipulation since they are stored on servers that are under the authority of CSPs but located outside of the hospital. To solve this security issue, we need strong cryptographic technologies and granular access control frameworks in third-party clouds. By fewer security and privacy issues in cloud computing, such as data loss, data alteration, and data breaches, the research goal in this work is to improve the security of electronic health records and maintain their privacy. Therefore, this study's key contribution and focus are as follows:

1) A demonstration of a protected Patient's Medical Electronic Health Records Management System (PRMS) offered by a third-party service provider and hosted in the cloud.

2) Implementing a web application prototype hosted on a third-party cloud service provider to implement a cloud-based, personalised steganographic encryption method for storing electronic medical records.

3) Implementing a web application prototype hosted on a third-party cloud service provider to implement a cloud-based, personalised steganographic encryption method for storing electronic medical records.

4) The system execution time and average delay of the suggested PRMS approach and the SRHB approach are compared.

5) Create a communication and data-acquisition model for cloud-based dispersed e-healthcare situations.

6 No other cloud platform has ever been compared to Fabric.

7) The user transactions counted, latency, and throughput are the main performance matrices.

To achieve the long-term goal of healthcare digitalization, which includes improving patient safety, quality, and efficiency while reducing the cost of healthcare delivery, both electronic medical records (EMRs) and electronic health records (EHRs) are very essential. Cloud storage, administration, security, sharing, and archiving can be useful for laboratory information systems, Electronic Health Records (EHRs), pharmaceutical information systems, and medical imaging. Due to current health records and ongoing interactions with multiple healthcare specialists, patients will generally receive good care. A third-party cloud presents a number of security difficulties and issues. like

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

any IT application. It frequently functions in a shared and open environment, making it vulnerable to theft, data loss, and hostile attacks. One of the main obstacles to full cloud adoption in the healthcare industry is a lack of cloud security. One of the numerous factors contributing to healthcare professionals' dread of the cloud is the challenge of giving up custody of their patients' medical records. Data is frequently stored by cloud service providers in a number of different data centres across the world. A clear advantage of having data stored globally is that cloud data storage would be redundant, several data centres will help in the event of a disaster, and disaster recovery is a huge benefit However, this same advantage could pose a security issue because data stored in multiple locations is more likely to be stolen or lost. Because they contain patient identification and extremely sensitive data, EHR are typically private and secret. On the other side, users of cloud computing services don't actually control their data. Furthermore, it is risky to fully rely on cloud service providers. Data loss can be devastating since it is difficult to know where, how, and when data is handled. This makes it difficult to verify the service provider. Therefore, when keeping health details in the cloud, individuals cannot completely trust third parties. E-health records kept in a third-party cloud must be protected with double-layer security in order to maintain their privacy and security.

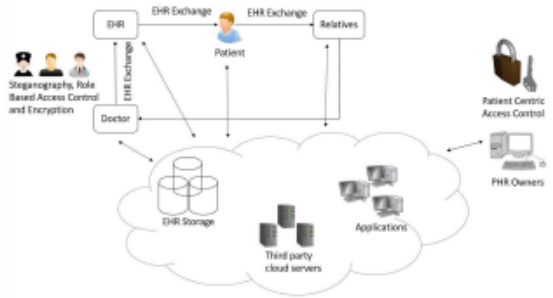

FIGURE 1. High-level general overview of cloud-based electronic health records.

OBJECTIVE:

By fewer security and privacy issues in cloud computing, such as data loss, data alteration, and data breaches, the research goal in this work is to improve the security of electronic health records and maintain their privacy.

SCOPE OF PROJECT

High-level general overview of cloud-based electronic health records. The project's scope is customers who use cloud computing services, on the other hand, do not have physical control over their data. Furthermore, it is risky to fully rely on cloud service providers. Data loss can be devastating since it is difficult to know where, how, and when data is handled. This makes it difficult to verify the service provider and causes a lack of transparency. Therefore, when keeping health details in the cloud, individuals cannot completely trust third parties. E-health records kept in a third-party cloud must be protected with double-layer security in order to maintain their privacy and security.

3. LITERATURE SURVEY

MUVINE: Multi-stage virtual network embedding in cloud data centers using reinforcement learning-based predictions.

The recent advances in virtualization technology have enabled the sharing of computing and networking resources of cloud data centers among multiple users. Virtual Network Embedding (VNE) is highly important and is an integral part of the cloud resource management. The lack of historical knowledge on cloud functioning and inability to foresee the future resource demand are two fundamental shortcomings of the traditional VNE approaches. The consequence of those shortcomings is the inefficient embedding of virtual resources on Substrate Nodes (SNs). On the contrary, application of Artificial Intelligence (AI) in VNE is still in the premature stage and needs further investigation. Considering the underlying complexity of VNE that includes numerous parameters, intelligent solutions are required to utilize the cloud resources efficiently via careful selection of appropriate SNs for the VNE. In this paper, Reinforcement Learning based prediction model is designed for the efficient Multi-stage Virtual Network Embedding (MUVINE) among the cloud data centers. The proposed MUVINE scheme is extensively simulated and evaluated against the recent state-of-the-art schemes. The simulation outcomes show that the proposed MUVINE scheme consistently outperforms over the existing schemes and provides the promising results.

RENDA: Resource and network aware data placement algorithm for periodic workloads in cloud

The Hadoop enabled cloud platforms are gradually becoming preferred computational environment to execute scientific big data workloads in a periodic manner. However, it is observed that the default data placement approach of such cloud platforms is not the efficient one and often ends up with significant data transfer overhead leading to degradation of the overall job completion time. In this article, a Resource and Network-aware Data Placement Algorithm (RENDA) is proposed to reduce the non-local executions and thereby reduce the overall job completion time for periodic workloads in the cloud environment. The entire job execution is modeled as a two-stage execution characterized as data distribution and data processing. The RENDA reduces the time of the stages as mentioned

above by estimating the heterogeneous performance of the nodes on a real-time basis followed by careful allocation of data in several installments to participating nodes. The experimental results show that the proposed RENDA algorithm consistently outperforms over the recent state-of-the-art alternatives with as much as 28 percent reduction in data transfer overhead leading to 16 percent reduction in average job completion time with 27 percent average speedup on average job execution.

Introducing cloud-assisted micro-service-based software development framework for healthcare systems

In healthcare services, application development is considered the most complex and time-consuming phase. As it is difficult to plan and time-intense, it requires high maintenance. Healthcare applications need strict compliance and the scope of application is immense along with associates, classes in services, and classified system. Application designing in healthcare with the help of traditional approaches such as monolithic and service-oriented architecture (SOA) generates problems in different areas like service availability, remote access to services, service provisioning, scalability, healthcare systems integration with each other. That is why there is a need for less sophisticated and user-friendly healthcare systems, which are easy to plan and develop, inexpensive requirement maintenance, and agile testing. To overcome the aforesaid issues in the domain of healthcare application development, this paper develops a framework of micro services for the development of healthcare services using cloud computing infrastructure. Micro-service-based techniques provide lightly coupled and fine-grained methodology. With the use of micro services technique presented in this work, the efficiency, scalability, and performance are improved. In this research, an approach for development and deployment properly in the cloud for healthcare applications is developed. Thus, it contributes to the system design approach and system analysis. Quantitative and qualitative results are reported showing the advantages of micro services approach used.

Edge intelligence and Internet of Things in healthcare: A survey

With the advent of new technologies and the fast pace of human life, patients today require a sophisticated and advanced smart healthcare framework that is tailored to suit their individual health requirements. Along with 5G and state-of-the-art smart Internet of Things (IoT) sensors, edge computing provides intelligent, real-time healthcare solutions that satisfy energy consumption and latency criteria. Earlier surveys on smart healthcare systems were centered on cloud and fog computing architectures, security, and authentication, and the types of sensors and devices used in edge computing frameworks. They did not focus on the healthcare IoT applications deployed within edge computing architectures. The first purpose of this study is to analyze the existing and evolving edge computing architectures and techniques for smart healthcare and recognize the demands and challenges of different application scenarios. We examine edge intelligence that targets health data classification with the tracking and identification of vital signs using state-of-the-art deep learning techniques. This study also presents a comprehensive analysis of the use of cutting-edge artificial intelligence-based classification and prediction techniques employed for edge intelligence. Even with its many advantages, edge intelligence poses challenges related to computational complexity and security. To offer a higher quality of life to patients, potential research recommendations for improving edge computing services for healthcare are identified in this study. This study also offers a brief overview of the general usage of IoT solutions in edge platforms for medical treatment and healthcare.

Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review

Cloud computing offers an innovative method of delivering IT services efficiently. Extant literature suggests that cloud technology can enhance the level of services in various industries, including healthcare services. As with any technological innovation, cloud computing should be rigorously evaluated before its widespread adoption. This research study presents a systematic review of scholarly articles of cloud computing in the healthcare sector. We considered 316 articles and filtered down to 88 articles to present a classification framework that has three dimensions: cloud computing-enabled healthcare opportunities, issues, and applications. Implications to future research and practice are highlighted in the areas of value-added healthcare services towards medical decision-making, data security & privacy obligations of cloud service providers, health monitoring features and innovative IT service delivery models using cloud computing.

Cybersyndrome and its formation, classification, recovery and prevention

There volutionary change in information and communication technology has made the people'slives much convenient more than ever before. But it has affected the human's physical and mental health as well as community's social connectivity. Cyber syndrome is the physical, social, and mental disorders that affect the human being due to the excessive interaction with the cyberspace. Many previous works have discussed the role that the technology plays in the development of

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

specific disorders, such as Internet addiction disorder or gaming addiction disorder. However, none of these works have explored the effects of excessive interaction with the cyberspace on the people's lives as a whole and its impact on the social connectivity of the community. Therefore, in this paper, we have presented the formation stages, classification, recovery, and prevention methods of cyber syndrome. We have explored the impact of cybersyndromein physical, social, and thinking spaces and its future implications and complications

4. MODULES

I. DOCTOR

Each doctor keeps a detailed register. The hospital gives the doctor authorization. Patients seek approval from doctors as well. Doctors are scheduled to see a patient. The report was uploaded by the doctor. A doctor and patient are having a live consultation. The doctor has a patient file.

II. PATIENT

Each patient has a registration with all of their information. Patient is logged in. The patient requests permission from the doctor. Dr. has given his approval. The patient is scheduled to see a doctor. Patient has uploaded a report about their illness. The doctor and patient are available live for the patient's comfort. A database of the patient's past records is kept.

III. HOSPITAL

A register with an ID and password is kept at the hospital. All doctor lists are in the hospital. Doctor requests are at the hospital.

IV. RELATIVE

The Relative has a login and user id register. A third party can view a relative's patient lists. Patient records are kept by a relative.

(a)PROPOSED ALGORITHM

Steganography AES Based Encryption

The art of steganography is the concealment of information in other data in a way that is invisible to the observer. The symmetric encryption technique AES (Advanced Encryption Standard) is frequently employed to protect digital data. We are utilising symmetric encryption in our project. The same key is used for both encryption and decryption in symmetric encryption, commonly referred to as private-key encryption. This means that for secure communication to occur, both the sender and the recipient of the material must possess the same secret key. However, because the key must be shared by both parties, symmetric encryption methods are less secure than asymmetric encryption algorithms.

The following steps are involved in the steganography AES-based encryption algorithm:

Encryption: The data that has to be hidden is first encrypted with a secret key using the AES method. Between the sender and the receiver, the key must remain a secret.

Decryption: The receiver must first separate the encrypted data from the cover data in order to be able to decrypt the concealed data. Using the same secret key that was used to encrypt the data, the retrieved data is then decrypted.

Since the data is encrypted, this AES-based steganography algorithm offers a high level of data protection. The approach is not entirely secure, though, as it is feasible for an attacker to determine whether data is present. In order to make the data harder to hack, extra methods like randomization might be implemented.

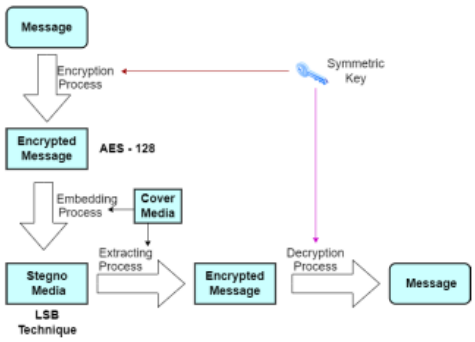

FIGURE 2. Securing data using steganography and encryption

Pseudo Code Algorithm

Algorithm 1

Combining AES – 128 Algorithm With Steganography

Input: E-Health Records (EHR), Cipher Key K.

Output: Cipher Health Record (CHR) stored in data over third-party cloud database

Create a key expansion of K that generates two lists of all sub keys.

Consider Partition EHR into 16-byte.

for Bi block do

Divide Bi into two arrays of 4 × 4 size

Perform Nine rounds manipulation following steps shown from

Step 6 to Step 9 6 Substitute bytes using predetermined e-healthcare table.

Shift rows.

Mix columns.

Add round keys.

Array out the tenth and final round of state manipulation.

Consider a copy of the final State array as the encrypted information (ciphertext) CHR.

Convert the CHR from binary to decimal.

Select cover image C1.

Apply encoder to C1.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

Calculate of each pixels of cover image.
Replace of cover image with each bit of secret message one by one.
Write stegano image.
Return the stegno-ciphered image.
Store stegano image in third party cloud database.
end

5. SYSTEM ARCHITECTURE

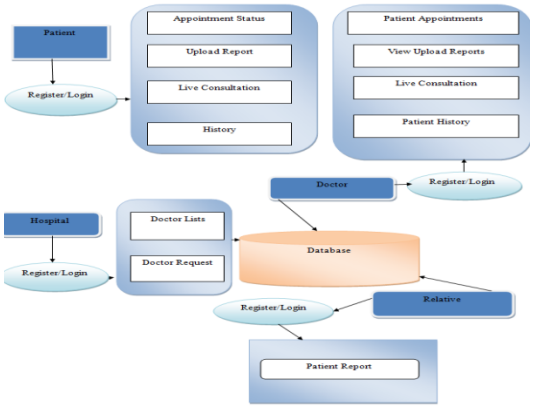

Figure 3: Architecture

The suggested PRMS system architecture is created with patient security as its sole goal. The doctor must include all the details. A hospital database was exchanged. A registration in the hospital contains all the information and logins. The hospital must approve a doctor before they are included to their list of doctors. A doctor will request it. The hospital has granted authorization to the doctor. The doctor has appointments with patients. Reports are viewable by the doctor. Doctor and patient have in-person consultations during which they communicate via messaging and go over reports. The doctor has a list of patients. Patient logs in after having a register filled out completely. Patient is taking a scheduled appointment. Reports are uploaded by the patient. The patient also receives a live consultation. The patient has a past.

6.SNAPSHOTS

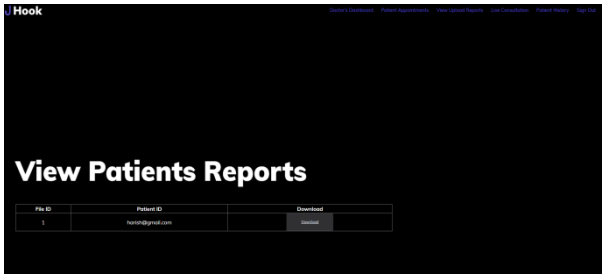

Fig 7.1 Doctor View Patient Report

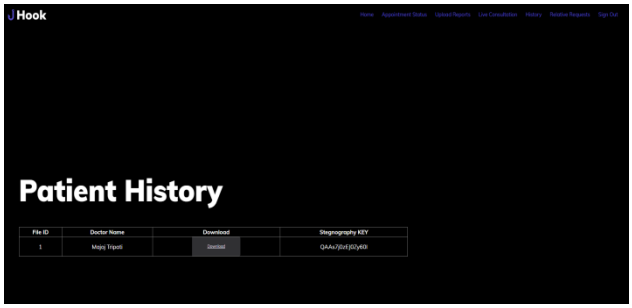

Fig 7.2 Patient History Page

Fig 7.3 Relative Patient Report

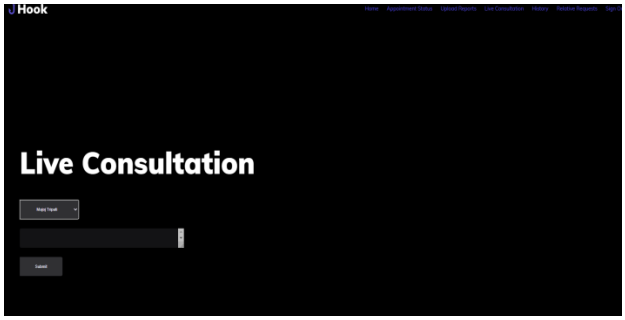

Fig 7.4 Patient Live Consultation

7.CONCLUSION

The efficiency of steganography encryption in a cloud setting is investigated in this article by contrasting platforms for throughput and latency fabric with different quantities of transactions. Ensuring the security of patient e-health records in the cloud is a serious concern. In terms of System Execution Time (SET) and Average Delay, the suggested PRMS (Patient Medical Records Management System) is contrasted with the Secure and Robust Healthcare-based method (SRHB). Maintaining user privacy, efficient medical data sharing, and information masking are just a few of the many quality matrices that contribute to the efficiency of the proposed PRMS design. PRMS is a security architecture that enables patients to manage their own health data while using encryption and steganography to secure patient health records in a third-party cloud from unauthorized access. The full system was built, and the article describes some of the system design for the PRMS cloud-based e-health application. Every evolved architecture has room for development. For improved

outcomes, additional obscuring and cryptographic methods can be introduced to the PRMS in the future.

(a)FUTURE WORK

To further improve the security of patient data stored in the cloud, future work will involve integrating data encryption and cloud storage security methods into the PRMS system. Future data security and privacy assessments will focus on external access to e-healthcare data transported over numerous networks.

8. 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.