IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v18.i4.pp62-72

Vol. 18 , Issue 4, 2022

Improving Patient Data Security and Privacy in Mobile Health Care: A Structure Employing WBANs, Multi-Biometric Key Creation, and Dynamic Metadata Rebuilding

Durga Praveen Deevi,
Software Quality Assurance Engineer,
O2 Technologies Inc., Irvine, CA, USA.
Email ID: durgapraveendeevi@gmail.com

ABSTRACT

Rapid technological advancements in mobile health (m-health) have transformed healthcare services, increasing their efficacy and efficiency. However, there are concerns to patient data security and privacy when cloud computing and m-health are combined. In order to overcome these obstacles, this study suggests a safe framework for mobile healthcare that makes use of Wireless Body Area Networks (WBANs) and a multi-biometric key generation technique. For scalable data processing and storage, the framework makes use of cloud computing platforms, guaranteeing dependability and flexibility. The Discrete Wavelet Transform (DWT) is used to extract features from electroencephalogram (EEG) and electrocardiogram (ECG) signals, which aid in key generation and improve security. Furthermore, hospital community clouds' electronic medical records (EMRs) are protected by dynamic metadata reconstruction, which guarantees legal compliance with privacy regulations. With regard to inter-sensor communication and cloud storage privacy, the suggested framework fills the vacuum in the literature by offering extensive security safeguards. The framework prevents risks related to data transmission and storage by providing end-to-end patient information protection using a mix of dynamic metadata reconstruction and multi-biometric key creation. By providing a solution that not only enhances the functionality of mobile healthcare services but also protects sensitive patient data, the study underscores the urgent need for increased security in the convergence of m-health and cloud computing, supporting the creation of safe and effective healthcare delivery systems.

Keywords: Mobile health (m-health), Wireless Body Area Networks (WBANs), Multi-biometric key generation, Dynamic metadata reconstruction, Electroencephalogram (EEG), Electrocardiogram (ECG), Discrete Wavelet Transform (DWT), Electronic medical records (EMRs), Security measures.

1. INTRODUCTION

The swift progress of mobile health (m-health) technology has brought about a substantial transformation in the healthcare services sector, augmenting its efficacy and efficiency. Numerous

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72

Vol. 15 , Issue 4, 2022

advantages arise from the combination of cloud computing and m-health, including enhanced contextual information consumption, energy savings, performance, and dependability. Nevertheless, additional security and privacy risks pertaining to patient data are also brought about by this connection. This research suggests a multi-biometric key generation strategy with Wireless Body Area Networks (WBANs) to create a secure framework for mobile healthcare in order to overcome these issues. This article examines the creation and application of this framework, offering a thorough examination of its elements, goals, and the gaps in the literature it seeks to address.

The use of wireless technology and mobile devices to handle patient data and provide healthcare services is known as mobile healthcare, or m-health. Due to its ability to offer real-time monitoring, remote consultations, and access to electronic health records (EHRs), m-health has become more popular during the last ten years. The emergence of cloud computing has contributed to the advancement of m-health by providing scalable storage options, easy access to data, and increased processing capacity. But in order to safeguard patient privacy and stop illegal access, strong security measures are required due to the sensitivity of healthcare data.

Scalability and flexibility are ensured by the suggested framework's utilization of cloud computing platforms for data processing and storage. Discrete wavelet transform (DWT) is included into the framework to extract features and quantize electrocardiogram (ECG) and electroencephalogram (EEG) signals. In addition, secure keys for inter-sensor communication are generated using a customized KeyGen technique. Additionally, the architecture makes use of hospital community clouds to store electronic medical records (EMRs) securely.

Researchers focused on improving data security in sensor-cloud infrastructure and subsequently built a safe cloud-based framework for mobile healthcare. Comprising two primary parts, the framework safeguards intersens or communication through a multi-biometric key generation technique and preserves patient privacy in cloud storage through a dynamic metadata reconstruction. Data breaches are reduced by the framework's integration of these elements, which guarantees the secure transmission and storage of sensitive healthcare data.

Developing a secure framework for mobile healthcare that tackles the issues of data security and privacy is the main goal of this project. The particular goals consist of:

Our proposal is a multi-biometric key generation technique for Wireless Body Area Networks (WBANs) to ensure inter-sensor communication security. Ensuring patient data privacy through dynamic metadata reconstruction is part of this, as is putting in place a secure storage solution for Electronic Medical Records (EMRs) within hospital community clouds. To further assist sensor-cloud infrastructures, we also offer guidance for privacy and security criteria. The integrity of the data is protected by our method, which strikes a balance between user privacy, administrative rights, and computing efficiency.

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72
Vol. 15 , Issue 4, 2022

The application of thorough security frameworks that handle inter-sensor communication and cloud storage privacy is conspicuously lacking, even in light of the advances in m-health and cloud computing. Current solutions seldom combine the two in a coherent way; instead, they usually concentrate on one component, such as safeguarding stored data or securing communication methods. The objective of this study is to close this gap by putting up a comprehensive framework that ensures end-to-end patient information protection from data transmission and storage security.

Ensuring the security and privacy of patient data is a critical concern when integrating m-health with cloud computing. The intricate risks connected to sensor-cloud architecture are frequently not sufficiently addressed by the security procedures in place. The findings of this study highlight the vital requirement for a strong security architecture that guards patient data while it is being sent and stored, preventing illegal access and data breaches. In order to address these issues comprehensively and advance safe and effective mobile healthcare services, the suggested multi-biometric key generation scheme and dynamic metadata reconstruction are being presented.

Finally, this study discusses the critical need for increased security measures in the combination of m-health and cloud computing. The study proposes a secure architecture combining WBANs, multi-biometric key generation, and dynamic metadata reconstruction to address the difficulties of patient data privacy and security. This framework not only enhances the dependability and performance of mobile healthcare services, but it also protects sensitive patient information, opening the way for more secure and efficient healthcare delivery systems.

2. LITERATURE REVIEW

Al-Muhtadi et al. (2019) study explores the privacy and cybersecurity issues that arise for mobile health apps that use social media in a multi-cloud setting. It draws attention to how crucial it is becoming to protect sensitive data using customized privacy settings and safe communication methods. The security and privacy of user data in mobile healthcare apps has become critical due to the increase in social media-driven information sharing. Users interacting with these apps must be able to adjust their privacy settings in order to allay these worries. Additionally, improving security protocols in cloud-to-cloud communications can greatly improve data security, particularly in medical settings.

In their study work, Sajid and Abbas (2016) address privacy concerns related to patient data in cloud-based healthcare systems. By means of an organized evaluation of the literature, they reveal that current approaches do not fully address these issues, which calls for increased efforts. The intention is to direct future research toward developing strong and fair privacy policies designed for these kinds of technologies. The Internet of Things (IoT) and cloud computing are two new technologies that are required for the integration of Wireless Body Area Networks (WBANs) in healthcare infrastructures. This combination brings up important questions about the privacy of private medical data. The comprehensive assessment of literature examines privacy concerns

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72

Vol. 15 , Issue 4, 2022

related to cloud-based healthcare systems. Results highlight the shortcomings of current privacy solutions and the need for improved approaches.

A new method for the safe and effective exchange of private health information in mobile healthcare social networks (MHSNs) is presented by Jiang et al. (2015). By using attribute-based encryption (ABE) and contracting out the decryption process to the cloud, their approach ensures the privacy of data and policies and permits fine-grained access control. By addressing security and privacy issues related to the exchange of personal health information among MHSNs, this program gives patients more control over their information. Furthermore, the addition of the Bloom filter improves privacy protection by enabling specific access controls for the sharing of PHI in MHSNs.

Yin et al. (2019) explore how IoT is being integrated into healthcare and the security issues that come with it, such as compromised patient data and data breaches. They put out an algorithm that is intended to protect user privacy by anonymizing private health data that is shared in an Internet of Things setting. The algorithm's effectiveness in guaranteeing safety in healthcare communication networks during IoT integration is mathematically demonstrated.

For e-healthcare cloud systems, Lin (2018) present a secure authentication and key agreement approach that enables anonymous authentication and does away with the requirement for a password table. This innovative method maintains user anonymity and ensures crucial security protocols while lowering computational expenses and manageme

Electronic health records (EHRs) are being shared more widely across healthcare practitioners in collaborative eHealth environments, but security and privacy continue to be major obstacles. Sánchez-Guerrero et al. (2017) suggest a privacy-aware profile management strategy as a solution to this. By combining user-generated claims and healthcare providers into a single credential, this gives patients more authority. The strategy attempts to protect sensitive EHR data while improving healthcare quality and cutting costs. The efficacy of this method is validated experimentally through simulated experiments.

The importance of mobile healthcare (mHealth) in improving healthcare access and treatment is emphasized by Wazid et al. (2017). They emphasize mHealth as a method that allows for ubiquitous access to health data and continuous medical care, made possible by mobile and patient monitoring equipment. A taxonomy of security procedures specifically designed for mHealth systems is presented in the article, which is essential for preventing threats and attacks. Even with the latest developments, there are still difficulties in creating mHealth systems that are reliable, safe, and affordable. Reaching the full potential of mHealth in revolutionizing healthcare delivery requires addressing these obstacles.

Kumar et al. (2018) highlight the sensitivity of medical data and call for stronger security measures in Telecare Medicine Information Systems (TMIS) in cloud computing environments. They point

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72

Vol. 15 , Issue 4, 2022

out weaknesses in the mutual authentication system currently in use for TMIS, including attack and session key compromise vulnerabilities. In order to tackle these issues, they present a new mutual authentication mechanism that provides enhanced security and computational effectiveness. The efficacy of the protocol is confirmed by formal assessments and security evaluations based on the random oracle model, demonstrating its resilience in protecting TMIS against different attacks.

Zeadally et al. (2016) investigate how vulnerable E-health systems are to cyberattacks, emphasizing the importance of recent assaults and suggested defenses. They recognize the increased susceptibility of Electronic Health (E-health) systems to data breaches and cyberattacks, but they also highlight the revolutionary power of ICTs in promoting E-health systems. The paper highlights how important it is to have strong security mechanisms in place in E-health systems to protect patients' private health information. Furthermore, it foresees difficulties that system designers and implementers will face in the future as e-health systems continue to interact with other technologies, requiring proactive steps to effectively fight developing risks.

A multi-tier cloud infrastructure is suggested by Quwaider and Jararweh (2016) as a means of creating a trustworthy global health awareness system designed to identify and forecast epidemic disease outbreaks. They draw attention to how urgently such a system is needed in view of current global health issues. The paper explores the challenges of building such a system, including limited resources, infrastructural constraints, and the need for international collaboration. It becomes clear that using cloud computing services is a workable plan to deal with these issues. In order to expedite health data sharing and reduce delays, the authors describe the deployment of a multi-tier cloud system that is enhanced by a mixed-integer optimization formulation. They show encouraging outcomes in terms of improving efficiency within the suggested framework.

IoT integration in healthcare is covered by Yin et al. (2019), along with the security threats that could arise from it, including patient data compromise and data breaches. Their study offers an algorithm to guarantee user privacy when exchanging sensitive health data in an IoT setting. This program successfully ensures safety in healthcare communication networks by incorporating a secure encryption mechanism and has been tested through mathematical analysis. IoT integration in healthcare has the ability to raise standards for effectiveness, safety, and quality of care, but it also raises security concerns.

A scoping review by Griebel et al. (2015) looks at how cloud computing is used in healthcare outside of traditional sectors. After analyzing 102 papers, they pinpoint six major areas and draw attention to the dearth of effective applications. Adoption in the healthcare sector is still heavily influenced by concerns about data security and safety. The field of cloud computing in healthcare is expanding quickly and presents opportunities for innovative approaches to service development, delivery, and utilization. Although "OMICS-context" applications are the main focus of the current study, there is potential for other uses. Telemedicine, medical imaging, patient self-management

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72

Vol. 15 , Issue 4, 2022

and public health, hospital administration and information systems, therapy, and secondary data utilization are among the primary study subjects. Although there is enthusiasm, there aren't many successful implementations at the moment, and there are still worries about the security and protection of data when working with outside cloud partners.

3. METHODOLOGY

3.1. Framework Design and Components

There are two primary parts to the suggested secure cloud-based system for mobile healthcare using WBANs:

Multibiometric Key Generation (M-BKG): One essential element intended to improve the security of intersensor communication systems is multibiometric key generation, or M-BKG. Its main purpose is to use biometric data to generate a secure key. Since biometric information—such as fingerprints, iris patterns, or facial features—is specific to each person, it is the perfect foundation for safe authentication. Using its uniqueness, M-BKG creates cryptographic keys that are used to encrypt and decrypt data sent back and forth amongst various sensors or devices connected to a network. M-BKG further improves security by adding more biometric modalities, which increases the produced keys' complexity and makes them more resilient to attempts at decryption or unwanted access. This technology is essential for protecting private data and maintaining the integrity of communication channels in a variety of settings, such as government organizations, financial transactions, and access control systems.

Dynamic Metadata Reconstruction: To strengthen the security of electronic medical records (EMRs) stored in the cloud, dynamic metadata reconstruction is a crucial component. Its primary duty is to dynamically reconstruct metadata, protecting the integrity and privacy of private medical information. Managing and safeguarding these records requires the use of metadata, which is information about the EMR that includes things like timestamps, access logs, and data ownership. This part improves security by reducing the possibility of tampering, illegal access, and data breaches through the dynamic reconstruction of metadata. A number of variables, including user access rights, data usage trends, and system events, are taken into account while updating and encrypting metadata throughout this dynamic reconstruction process. By doing this, cloud-based EMR systems' overall security posture is strengthened and privacy laws like HIPAA are more easily complied with. This technology is essential for protecting patient privacy and guaranteeing the reliability of medical data in online settings.

3.2. Multibiometric Key Generation

Feature Selection and Extraction: Using the discrete wavelet transform (DWT), features from electroencephalogram (EEG) and electrocardiogram (ECG) data are retrieved and quantified. A signal can be broken down into its individual frequency components using the DWT signal

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72

Vol. 15 , Issue 4, 2022

processing approach, which makes it possible to extract pertinent information. The brain and heart activities are represented by the EEG and ECG signals, which are captured at a rate of 125 Hz, or 125 samples per second.

By dividing the signals into several frequency bands, the discrete wavelet transform captures information at both high and low frequencies. The derived wavelet coefficients are quantized, which provides the extracted characteristics in a digital format that can be used for additional processing and analysis. This method makes it possible to characterize significant patterns and changes in the EEG and ECG signals, which can be useful for a variety of purposes including medical monitoring, diagnosis, and research in disciplines like cardiology and neurology.

Key Generation: The quantized data is used to generate two keys, each with 160 bits, using the KeyGen algorithm. After that, these keys are joined together, or concatenated, to create a single key with 320 bits. By lengthening and complicating the encryption key, this method strengthens security and increases its resistance to brute-force assaults and other cryptographic flaws. The approach guarantees that the generated encryption key is based on relevant information collected from the original signals by constructing keys from the quantized data, which reflects digital copies of extracted features. This method preserves the data's confidentiality and integrity while enabling safe transmission or storage in a range of applications, including network security, cryptography, and data protection in industries including telecommunications, finance, and healthcare.

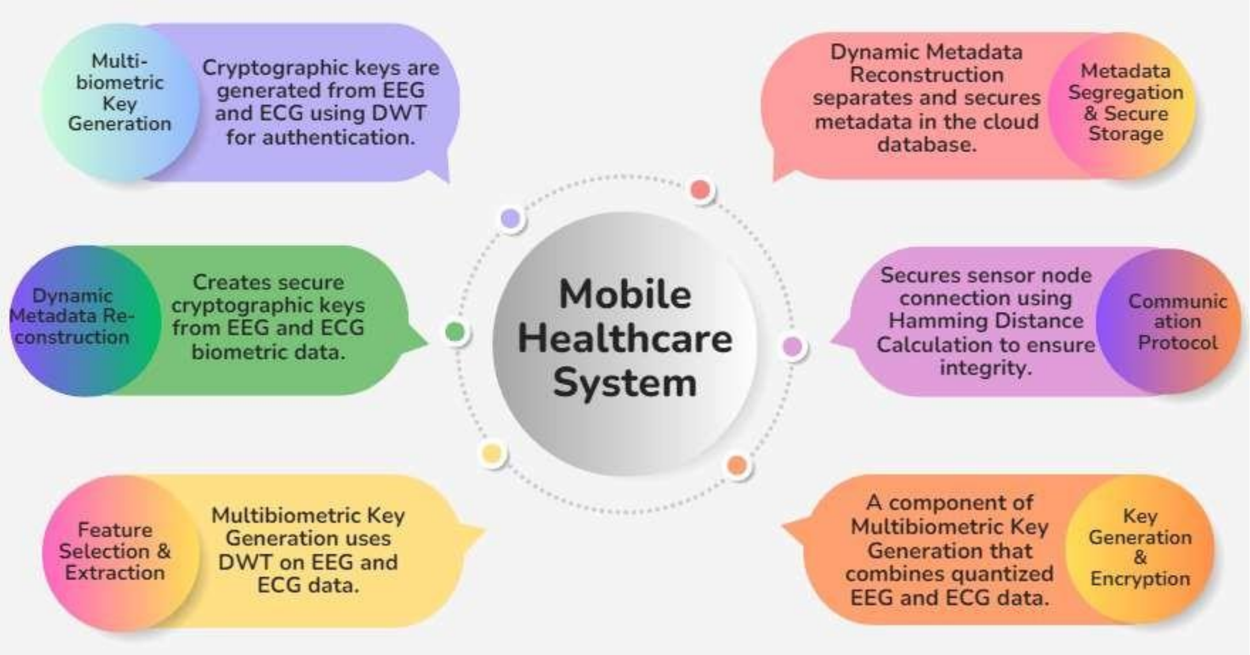
Multi-biometric Key Generation
Cryptographic keys are generated from EEG and ECG using DWT for authentication.
Dynamic Metadata Reconstruction separates and secures metadata in the cloud database.
Metadata Segregation & Secure Storage
Dynamic Metadata Re-construction
Creates secure cryptographic keys from EEG and ECG biometric data.
Mobile Healthcare System
Secures sensor node connection using Hamming Distance Calculation to ensure integrity.
Communic ation Protocol
Feature Selection & Extraction
Multibiometric Key Generation uses DWT on EEG and ECG data.
A component of Multibiometric Key Generation that combines quantized EEG and ECG data.
Key Generation & Encryption

Figure 1: Architecture of a Secure Cloud-Based Mobile Healthcare System.

Communication Protocol: Sensor node 'a' sends a 'Hello' message along with its unique identity (ID) to sensor node 'b' in order to open a communication channel. A matrix construction and the

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72

Vol. 15 , Issue 4, 2022

Hamming distance calculation method are used to guarantee the security of transmission. In order to make further operations easier, the data must be arranged into a structured format, such as a matrix, through the process of matrix creation. By calculating the amount of different bits between two strings of data, the Hamming distance calculation calculates the difference between them. The communication system can confirm the validity and integrity of the sent data by using this technique. By making it possible to identify any possible tampering or illegal access during transmission, this method improves security. These methods are widely used in many domains that need secure communication, like wireless sensor networks, Internet of Things (IoT) devices, and telephony, providing strong defense against hostile activity and data breaches.

3.3. Dynamic Metadata Reconstruction

Metadata Segregation: Divide and store metadata elements independently within the cloud database is a technique known as metadata segregation. By keeping critical metadata hidden and unlinkable from particular people or data, this technique protects user privacy. The cloud service provider can lower the danger of illegal access or data breaches by enforcing stronger access restrictions and encryption procedures through the segregation of metadata. While allowing for effective data management and retrieval within the cloud architecture, this method guarantees the protection of user privacy.

Secure Storage: Electronic medical records (EMRs) can be securely stored on the hospital community cloud. A framework is built to design database schemas specifically for maintaining privacy while storing metadata in the cloud, guaranteeing both efficiency and privacy. This method protects private patient data by making it easier to store electronic medical records in an orderly and secure manner. It also makes it possible for seamless integration with mobile healthcare solutions, guaranteeing that medical data may be handled and accessed securely on mobile devices while abiding by industry standards and privacy laws.

Table 1: Comparison of Security Techniques.

Technique	**Features**	**Benefits**	**Drawbacks**
Multibiometric Key Generation	Uses biometric data (ECG, EEG)	High security, random key generation	Computationally intensive
Dynamic Metadata Reconstruction	Segregates and stores metadata	Protects privacy, flexible storage	Complexity in implementation
Traditional Encryption	Uses standard encryption algorithms	Simple to implement	Lower security against advanced threats

Two-Factor Authentication	Combines password and secondary input	Enhanced security	User convenience issues

The table provides a comparison of the various security methods used in mobile healthcare. By classifying each approach according to its description, features, advantages, and disadvantages, it enables stakeholders to assess each one thoroughly. Techniques are explained in terms of the security measures they employ, whilst features draw attention to their special traits or elements. Benefits highlight each technique's advantages, such as increased user privacy or better data protection. On the other hand, disadvantages highlight restrictions or difficulties, such heightened complexity or possible weaknesses. By weighing the trade-offs of each security strategy, this comparative analysis helps stakeholders make well-informed decisions that are in line with their unique needs and limitations in mobile healthcare settings.

Eq: Hamming Distance Calculation

$$H(i,j) = \sum_{k=1}^{n} \square \, |x_{ik} - y_{jk}| \qquad (1)$$

Where:

- $H(i,j)$ is the Hamming distance between sensor 1's block iii and sensor 2's block jjj.
- x_{ik} and y_{jk} are the elements of the respective blocks.
- n is the number of elements in each block.

The equation calculates the Hamming distance $H(i,j)$ between two blocks of data i and j from different sensors. Here's a breakdown of the components:

- $H(i,j)$: This represents the Hamming distance between the ith block from sensor 1 and the jth block from sensor 2.
- $|x_{ik} - y_{jk}|$: This calculates the absolute difference between the kth elements of the two blocks.
- $\sum_{k=1}^{n} \square$: This symbolizes the summation over all n elements in each block.

In essence, the equation measures the dissimilarity or "distance" between the data blocks by summing the absolute differences of their corresponding elements.

The urgent requirement for improved security measures in sensor-cloud infrastructure is addressed by the suggested secure framework for mobile healthcare. Secure intersensor communication and the privacy of stored EMRs are guaranteed by the framework through the use of multibiometric key generation and dynamic metadata reconstruction. This all-encompassing strategy not only

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72
Vol. 15 , Issue 4, 2022

enhances the performance and dependability of mobile health services but also protects private patient data, opening the door to more effective and safe healthcare delivery systems.

5. CONCLUSION

In overall, a strong answer to the security and privacy issues arising from the combination of cloud computing with m-health is provided by the suggested framework. The framework enables safe patient data storage and exchange by combining dynamic metadata reconstruction with multi-biometric key creation. While respecting privacy laws, this all-encompassing strategy improves the effectiveness and dependability of mobile healthcare services. Putting such a framework into place is essential to promoting the adoption of safe and effective healthcare delivery systems in the digital era.

6. FUTURE SCOPE

Subsequent studies might investigate the performance and scalability of the suggested framework in practical mobile health apps. Furthermore, the security posture of mobile healthcare systems may be further strengthened by developments in biometric authentication methods and cloud security procedures. There may be new ways to improve patient data security and privacy in mobile healthcare settings by looking into how emerging technologies like blockchain and artificial intelligence can be integrated.

7. REFERENCE

1. Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. Health informatics journal, 25(2), 315-329.
2. Sajid, A., & Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of medical systems, 40(6), 155.
3. Jiang, S., Zhu, X., & Wang, L. (2015). EPPS: Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks. Sensors, 15(9), 22419-22438.
4. Yin, X. C., Liu, Z. G., Ndibanje, B., Nkenyereye, L., & Riazul Islam, S. M. (2019). An IoT-based anonymous function for security and privacy in healthcare sensor networks. Sensors, 19(14), 3146.
5. Lin, H. Y. (2018). A secure heterogeneous mobile authentication and key agreement scheme for e-healthcare cloud systems. Plos one, 13(12), e0208397.
6. Sánchez-Guerrero, R., Mendoza, F. A., Diaz-Sanchez, D., Cabarcos, P. A., & López, A. M. (2017). Collaborative ehealth meets security: Privacy-enhancing patient profile management. IEEE journal of biomedical and health informatics, 21(6), 1741-1749.

https://doi.org/10.62643/ijerst.2022.v15.i4.pp62-72

Vol. 15 , Issue 4, 2022

7. Wazid, M., Zeadally, S., Das, A. K., & Odelu, V. (2016). Analysis of security protocols for mobile healthcare. Journal of medical systems, 40, 1-10.
8. Kumar, V., Jangirala, S., & Ahmad, M. (2018). An efficient mutual authentication framework for healthcare system in cloud computing. Journal of medical systems, 42, 1-25.
9. Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (e-health) systems. Journal of medical systems, 40, 1-12.
10. Quwaider, M., & Jararweh, Y. (2016). Multi-tier cloud infrastructure support for reliable global health awareness system. Simulation modelling practice and theory, 67, 44-58.
11. Yin, X. C., Liu, Z. G., Ndibanje, B., Nkenyereye, L., & Riazul Islam, S. M. (2019). An IoT-based anonymous function for security and privacy in healthcare sensor networks. Sensors, 19(14), 3146.
12. Griebel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., ... & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. BMC medical informatics and decision making, 15(1), 1-16.