Design of Security and Privacy Framework for Medical Health Care System in IoT

Kamlesh Kumar Yadav[1], Dhablia Dharmesh Kirit[2]

[1]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
[2]Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.

The development of the Internet of Things (IoT) in recent years has fueled the emergence of smart e-health monitoring systems and services, which highlights the system's significance in the present healthcare environment. The notion of health monitoring has undergone significant change as a result of technological advancements. Patients' concerns and those of all other end users involved in the health care monitoring system will now give real-time updates on health conditions. Contributing a traditional method to the e-health monitoring system through the use of a fully intelligent system is one of the main criteria. The idea put forward here is to gather pertinent medical data from various sensors, sort through it to extract pertinent details about the patient's current condition, and then identify and incorporate the health status. An further significant issue that arises in hospital networks is the security and privacy of health information. It might occur when a hacker listens in on patient medical data while it's being transmitted; afterwards, he could misuse the information. Because the typical security system requires infinite resources, it is exceedingly challenging to deploy in the current environment. For this reason, privacy and security are especially crucial in applications related to health care. The planned effort exemplifies the traditional use of IoT in medical heath data, dedicated to an architecture and system devices.

Keywords: healthcare, medical environments, App, Security, Privacy, Trust.

1. Introduction

IoT expansion brings with it new security challenges as well as a worsening of existing ones. In order to empower ideas and techniques for remote monitoring, diagnostics, and other health-related activities, health care monitoring devices have been developed. Health monitoring ought to be an ongoing process that tracks a patient's condition and gives the medical staff information for diagnosis [1]. In an emergency, this will assist patients and the elderly without requiring hospitalisation. The majority of industrialised and developing nations lack adequate human resources in their healthcare systems; as a result, the general population needs a new type of health care system [3]. Because they are unable to walk about easily, senior citizens do not often visit the hospital; however, advanced techniques can be employed to send them best wishes. While the passive attack monitors the IoT network without affecting the services, the aggressive attack interrupts the services [9]. Every framework or solution for IoT privacy needs to handle the following issues. (1) Tracking and Profiling. Identity association with a specific person is a risk because it can result in tracking and profiling [2]. Therefore, prohibiting such behaviour in IoT and implementing certain preventive measures is one of the main issues. (2) Tracking and Localization. Another risk is localization, which arises when computers attempt to track and record a person's whereabouts over space and time. Creating standards for IoT interactions that discourage such behaviour is one of the main problems in developing security solutions for IoT. In e-commerce applications, it is common practice to use profile information about an individual to infer preferences through correlations with other profiles and data. A significant difficulty is striking a balance between user privacy regulations and company objectives in data analysis and profiling. (3) Safe Transmission of Data. Making sure that data are sent through public media in a safe manner, keeping information secret from others, is another security measure that helps stop illegal data collecting on objects and people. [11]. The protection of patient health information from various risks is the health care system's top responsibility.

The rest of the paper is organized as follows: Section 2 provides the classification scheme for the survey; Section 3 provides an overview of proposed architecture. Section 4 provides a summary and comparison of the results of the various papers discussed in this taxonomy. Finally, Section 5 concludes the paper.

2. Related Works

According to the work [4], which describes security and privacy of mobile health applications, 95.63% of these applications are vulnerable to security and privacy issues. A variety of mobile health applications gather sensitive health information. Since wearable technology gathers 30TB of health data on average, Internet of Things connectivity needs to be categorised, controlled, and safeguarded [6]. Since automation technology powers the majority of wearables, data security has also been compromised. AWS (Amazon Web Service) IoT, Azure IoT, and other IoT frameworks are included in [5], which provides an IoT framework for security and privacy. literature [4], which discusses several IoT threat levels, access control, verification, and security analysis. Energy harvesting and a lightweight security mechanism are recommended as solutions. The author of [12] discusses the design of IoT systems, privacy and security concerns, and the integration of CPS (Cyber Physical System) with IoT. CPS offers a vertically designed, isolated type of CPS without any connectivity, while IoT uses networking infrastructure to offer a resource for sharing [13].

In order to precisely design a treatment plan and diagnose the disease based on prior patient diagnosis results, machine learning can also be utilised to extract information from massive datasets. Sensor nodes and mobile devices lack the storage capacity and processing power necessary for machine learning, therefore cloud technology is required to do this. Cloud platforms, on the other hand, facilitate machine learning by offering large databases and significant computational power. Machine learning provides data on disease patterns, treatment plan formulation, and disease connectivity [7]. To achieve better results, classification algorithms can also be implemented on the cloud; however, there is no one best machine learning method; rather, some are appropriate for certain contexts but not for others.

3. Methodologies

The collection of algorithms that make up the unified strategy for maintaining security and privacy in the e-health care system is shown in Figure 1. The MEHR algorithm offers both a mobile application and a respectable architectural concept. In Figure 1, the patient registered with their home network, the Authentication Unit (AU) generated the Global Secret Key (GSK), and the medical node combined medial data to form MEHR. These records were encrypted using the MEHR algorithm, allowing the patient to define an update policy and extract keywords during the encryption process before being deposited in a cloud storage. The authorised user can only see and decrypt the medical record; if they would like to amend any information, they must utilise the key they created at registration.

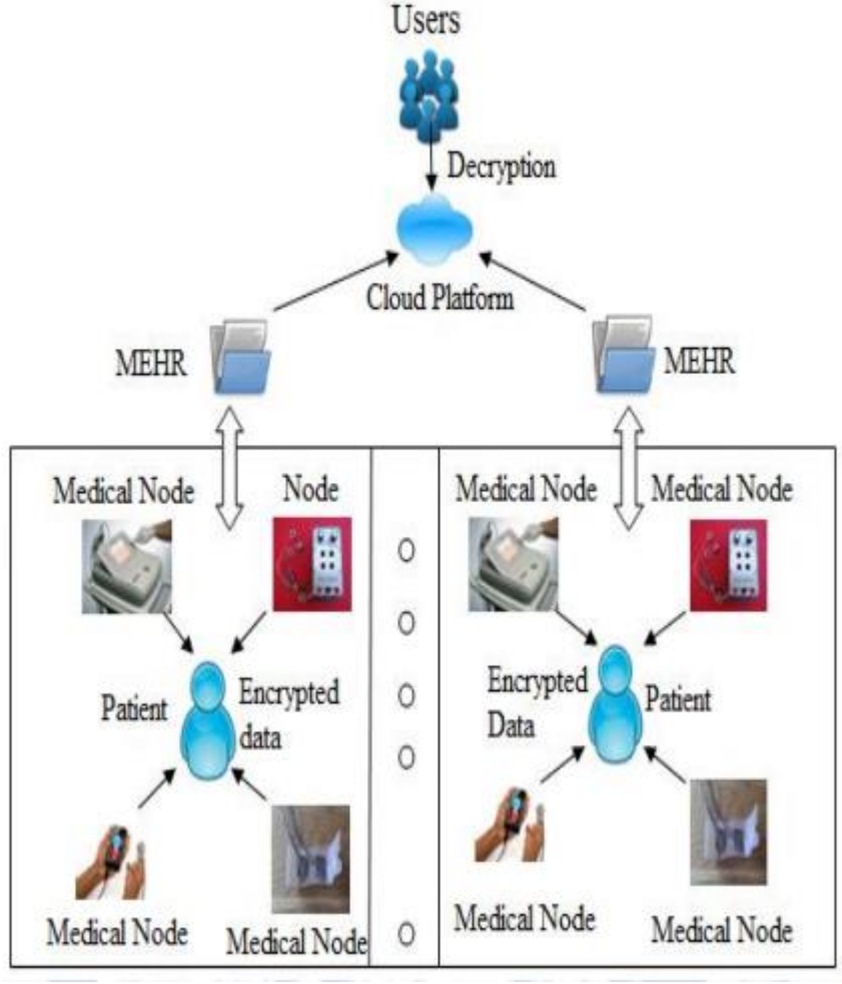

Figure 1: Resources influencing QoES Computation

The patient registration and GSK generation are completed in the step above, and the MEHR algorithm will offer a secure authentication method. Additionally, by sharing the secret key and private key, respectively, a secure environment will be created. A keyword match is performed when a patient uses the second algorithm to update their access to a medical electronic health record (MEHR) stored on a secure cloud platform. If the match is accepted, the update function will operate from the cloud platform [8].

Since real-time attacks are encountered in IEEE 802.11, security evaluation is crucial in the Internet of Things. Researchers have also addressed security difficulties in MANETs, such as the black hole attack. These assaults have an impact on the network's performance. In the part above, a detailed algorithm is mentioned to encounter security and privacy. Following that, a thorough security evaluation is described. The Health Insurance Probability and Accountability Act, or HIPAA, closely regulates every healthcare organisation to guarantee the security and privacy of patient data. Two key issues have come up during the examination of e-health data security and privacy: consistency and repeatability. For instance, smartcard security, which uses extremely advanced technology, also meets a wide range of attack parameters and types. In order to assess medical health information privacy and security in an environment, it can also be helpful to simulate an attack. However, in order to do so, realistic network traffic must be created, maintaining all of the features of real traffic [14].

4. Results and Discussion

Any system's performance needs to be monitored and evaluated in order to be improved; this requires quantification. The behaviour of IoT devices and networks, as well as patient perspectives, are the primary means of evaluating the efficacy of health monitoring. Different objectives and ambitions among stakeholders result in differing perceptions of performance across multiple dimensions and dynamics across time. The suggested system's simulation configuration is based on the simulation of current systems as described in [10]. A computer running 64-bit Windows 10 Professional, an Intel Core i5 processor or an equivalent with a 6700 2.4/5 GHz core CPU, and 8GB of RAM are included in the simulation setup. The pairing-based cryptography (PCB) library is used to run the simulation, and a mobile application is also created. The platform used to develop applications is called Android Studio.

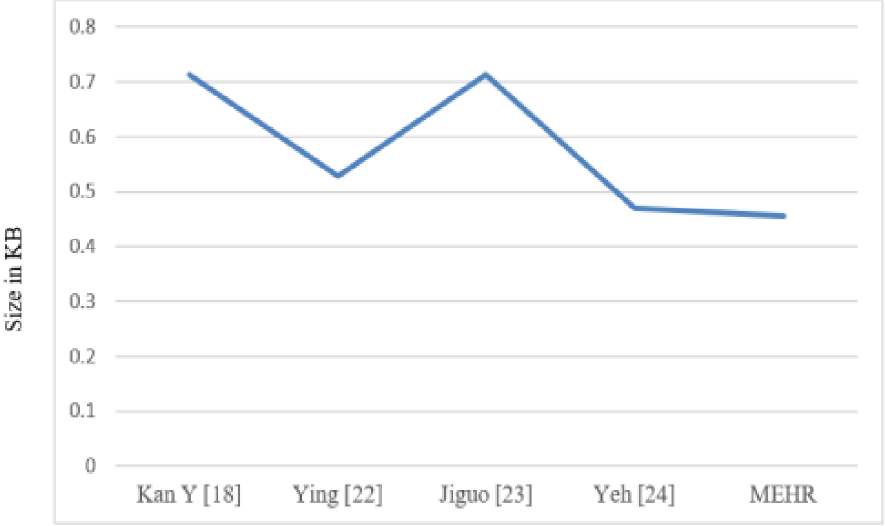

Figure 2: Transmission cost parameter

Figure 2 displays the cost of transmission, the number of parameters in the value of the x-axis diverge, and the cost of public parameters. The size of the public parameter in our system is

0.456KB, 0.528KB, 0.7.12KB, 0.469KB, and 0.712KB in the scheme.

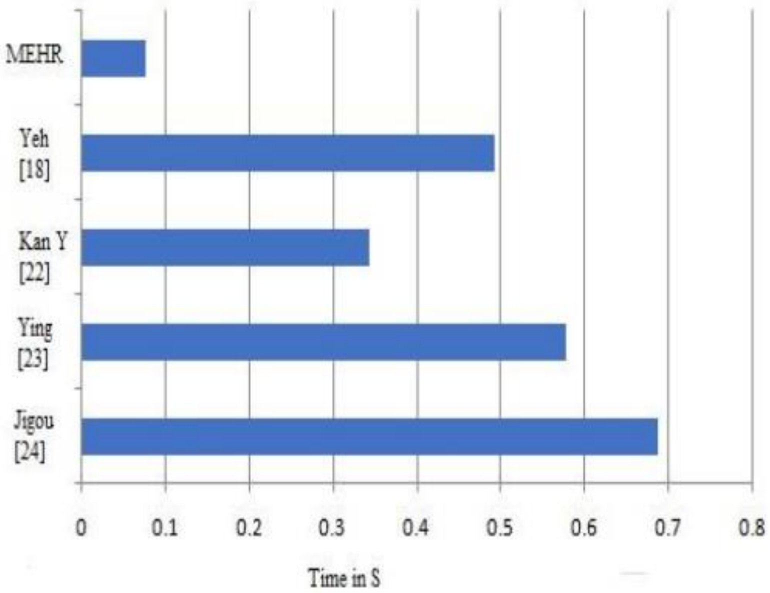

Figure 3: MEHR Encryption

Figure 3 compares the processing costs associated with encrypting medical files. The x-axis shows the computing cost, while the y-axis shows the various schemes and current work. 0.496, 0.342, 0.573s, 0.677s, and 0.687s collectively are the final figures; it is clear that the proposed system has the lowest computing cost. Data shared with several users can be challenging to share, and there are cryptographic techniques available to encrypt user data before it is shared. In health care applications, data de-identification occurs when identifiers are safeguarded; privacy regulations might also serve to protect this.

The microcontroller is used to calibrate the patient's health data, and medical sensors such as a temperature and humidity sensor, room temperature sensor, and heart monitor are installed in the monitoring apparatus. After security and privacy are ensured, this sensor data are transferred to a cloud database server, where health data can only be accessed by authorised individuals via an IoT application platform to prevent security breaches. The medical professional can diagnose the illness and recommend a course of therapy based on the information provided by a secure architecture and an intuitive mobile application. The doctor can give medication and urge medical treatment even when they are far away. Ultimately, a thorough comparison is conducted to demonstrate that the system outperforms every other system in use in the present sectors in terms of efficiency and security.

5. Conclusions

The system's design accomplishes the following goals: i) creates a secure architecture for the storage and transmission of medical data without jeopardising patient security and privacy; ii) guarantees the anonymity and traceability of both the medical node and the user; iii) includes a lightweight mechanism for updating policies; iv) offers a user-friendly interface or application that makes it simple for authorised users (who may include doctors and attendees) to access health records. In order to improve security and privacy in e-health care systems, it is necessary to detect and prevent all forms of attacks during installation in order to provide a secure environment for the Internet of Things. The MEHR algorithm also demonstrates how important it is for the suggested system to accomplish the goal; it satisfies every requirement for security, privacy, key management, access update, and interface.

References

1. Rana, Arun, Chinmay Chakraborty, Sharad Sharma, Sachin Dhawan, Subhendu Kumar Pani, and Imran Ashraf. "Internet of medical things-based secure and energy-efficient framework for health care." Big Data 10, no. 1 (2022): 18-33.
2. Awotunde, Joseph Bamidele, Rasheed Gbenga Jimoh, Sakinat Oluwabukonla Folorunso, Emmanuel Abidemi Adeniyi, Kazeem Moses Abiodun, and Oluwatobi Oluwaseyi Banjo. "Privacy and security concerns in IoT-based healthcare systems." In The fusion of internet of things, artificial intelligence, and cloud computing in health care, pp. 105-134. Cham: Springer International Publishing, 2021.
3. S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21
4. Karunarathne, Sivanarayani M., Neetesh Saxena, and Muhammad Khurram Khan. "Security and privacy in IoT smart healthcare." IEEE Internet Computing 25, no. 4 (2021): 37-48.
5. Islam, SK Hafizul, and Debabrata Samanta, eds. Smart Healthcare System Design: Security and Privacy Aspects. John Wiley & Sons, 2021.
6. Sonya, A., & Kavitha, G. (2022). A Data Integrity and Security Approach for Health Care Data in Cloud Environment. Journal of Internet Services and Information Security, 12(4), 246-256.
7. Kumar, Randhir, and Rakesh Tripathi. "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology." the Journal of Supercomputing 77, no. 8 (2021): 7916-7955.
8. Kalpally, Adarsh T., and K. P. Vijayakumar. "Privacy and security framework for health care systems in IoT: originating at architecture through application." Journal of Ambient Intelligence and Humanized Computing (2021): 1-11.
9. Malathi, K., Shruthi, S.N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P.M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 60-72. https://doi.org/10.58346/JOWUA.2024.I2.005
10. Kumar, S.Sunil, S.Parveen, and S.Benjamen Samuel. 2020. A Case Report on Erythema Multiforme (EM): Systemic and topical steroidal therapy, along with antibiotics. International Journal of Pharmacy Research & Technology, 10 (1), 5-8. doi:10.31838/ijprt/10.01.02
11. Sun, Yingnan, Frank P-W. Lo, and Benny Lo. "Security and privacy for the internet of medical things enabled healthcare systems: A survey." IEEE Access 7 (2019): 183339-183355.
12. Chakraborty, Sabyasachi, Satyabrata Aich, and Hee-Cheol Kim. "A secure healthcare system design framework using blockchain technology." In 2019 21st international conference on advanced communication technology (ICACT), pp. 260-264. IEEE, 2019.

13. Fazeldehkordi, Elahe, Olaf Owe, and Josef Noll. "Security and privacy in IoT systems: a case study of healthcare products." In 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), pp. 1-8. IEEE, 2019.
14. Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.
15. Butpheng, Chanapha, Kuo-Hui Yeh, and Hu Xiong. "Security and privacy in IoT-cloud-based e-health systems—A comprehensive review." Symmetry 12, no. 7 (2020): 1191.