Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 3345-3350

Secure Decision Support System in Medical Cyber Physical Network

Urmila[1], Mr. Sabir Ali[2], Dr. Sunita Chaudhary*[3]
[1]Marudhar Engineering College, Bikaner, Rajasthan
[2]Associate Professor, Marudhar Engineering College, Bikaner, Rajasthan
[3]Professor, Marudhar Engineering College, Bikaner, Rajasthan
ORCID ID:- 0000-0001-8913-4897
*Email:er.sunita03@gmail.com

ABSTRACT

Medical Secure Systems (MSSs) are characterized by integrating computation and physical processes. The theories and applications of MSSs Face the enormous challenges. The aim of this work is to provide a better understanding of this emerging multidisciplinary methodology. In this work we focused on the MSS in medical applications, which is known as Medical Secure Systems (MSS). In MSS, multiple data can be transmitting to the private or public cloud for storage and processing. Over these data, machine learning algorithms can be applied to process that data, which will be further useful to take some decisions for healthcare professional. This data can be sensitive and is publically available and provided to third party storage space, so that the challenging issue of security is arises. To provide the security, in this paper we applied cryptographic technique such as AES to encrypt the data before store on cloud servers. After this, to enhance the further security, we will use the concept of digital envelope. In this concept, data encryption AES key is again encrypted by using ECC encryption key. Again to reduce the key management overhead, system makes use of Key Distribution Center (KDC), which can generate and manage the keys for all users. Finally experimental results prove that, this MSS system is more secure than previous one and it is also reduce the key management overhead.

Keyword:- Medical Secure Systems ,Key Distribution Center, AES, encryption.

INTRODUCTION

Medical Secure Systems (MSS) research has lately piqued the interest of academics, business, and government officials because to its broad implications for society, economy, and environment. MSS are said to be the next generation of designed systems with the integration of communication, computing, and control to accomplish the objectives of stability, performance, resilience, and efficiency for MSS, despite the absence of a formal definition. While continuing research efforts are aimed towards attaining these objectives, MSS security is mostly disregarded. However, since MSS are extensively integrated in a variety of important infrastructures, any security breaches might have disastrous repercussions.

Accidents might occur if a vehicle to vehicle (V2V) communication network is hacked, for example, because incorrect distance information is supplied. In reality, the introduction of self-driving cars has exacerbated the issue since passengers must trust the vehicles' choices. The inexorable pace in the development of such devices paved the way for the creation of comprehensive patient health monitoring systems that may be used in clinical settings. An distributed sensor network may collect medical data from patients and send it to private or public cloud services. The association of patient data to known illness states may be determined using a collection of statistical inference algorithms operating in the cloud. These associations might be communicated back to medical professionals as a way to help them make decisions. MSS frameworks herald the start of a new Digital-Health (D-Health) era and a problematic invention in human history. Providing security for personas' health data that is transported to the cloud with the help of tangible systems, and from the cloud to medical expertise mobile phones, would necessitate the development of refined cryptographic designing procedures for MSS, as previously stated. As an alternative to the typical encryption plans and strategies recommended in this course of action, emerging cryptographic algorithms provide options for ensuring information exchange and secure figuring while also providing greater levels of security. The MSS has a seven-layer structure, with the layers being information procurement, information aggregation, cloud management, activity, AES encryption, KDC, and Digital Envelope, among other things.

Building the structural parts of MSSs, such as sensors, cloud computing structures, and rapid Internet and mobile phone connections, will need overcoming mechanical challenges. In practice, public clouds provide various benefits, including no chain of risk to infrastructure providers and no upfront investment expense. The public, on the other hand, lacks effective control over network, data, and security settings, which reduces interest in cloud services. They also exacerbate the problems of data security, privacy, and trust. The private cloud, on the other hand, reflects the service quality criteria such as dependability, security, and performance. Furthermore, ensuring the privacy of individual health data during transmission from sensory systems to the cloud and also from the cloud to physicians' mobile phones would need the development of a sophisticated cryptographic architecture for an MSS. While this strategy only recommends safe storage using traditional encryption techniques, newer encryption schemes provide possibilities for secure information transfer and processing.

The fundamental goal of this research is to have a better understanding of these new trans-disciplinary methodologies.

- Use AES to encrypt data before storing it on cloud servers.
- To improve security even further, the system will use the concept of a digital envelope.
- The ECC encryption key is used to derive the AES key for information encryption.
- Framework makes use of a Key Distribution Center (KDC) to decrease key management costs. The KDC may maintain keys for all users.

ARCHITECTURE

The following are detailed descriptions of the Architecture:

- **Read / Browse Dataset**

The user may browse the input dataset, which is based on patient medical data. The next sections go through the dataset in more detail.

- **Data Preprocessing**

Data preparation is carried out on the dataset. The dataset is first read, followed by the creation of a training file for the classification process.

- **Encryption of data**

The system uses the AES Algorithm to encrypt the data for security reasons. The steps of the AES algorithm and how it works are discussed in the algorithm sections.

- **Classification**

Classification is the process of identifying patient data in a decision support system. Initially, the doctor sends a request to the server for the purpose of identifying health data; the server's SVM classifier performs the classification process and returns the findings to the doctor; the doctor receives the data and decrypts it.

- **KDC**

KDC and TPA are involved in this system, and they do digital envelop and integrity checks, respectively. To begin, connect in to the cloud server and obtain a key from the KDC. Using the AES and ECC algorithms, KDC will generate a master key, as well as a pair of public and secret keys. The master key is then encrypted using the requested data owner's ECC public key, and the encrypted master key and secret key are sent to the data owner. After receiving the key, the owner of the data fragments the file into blocks, encrypts them using an encrypted master key, and sends them to the cloud server.

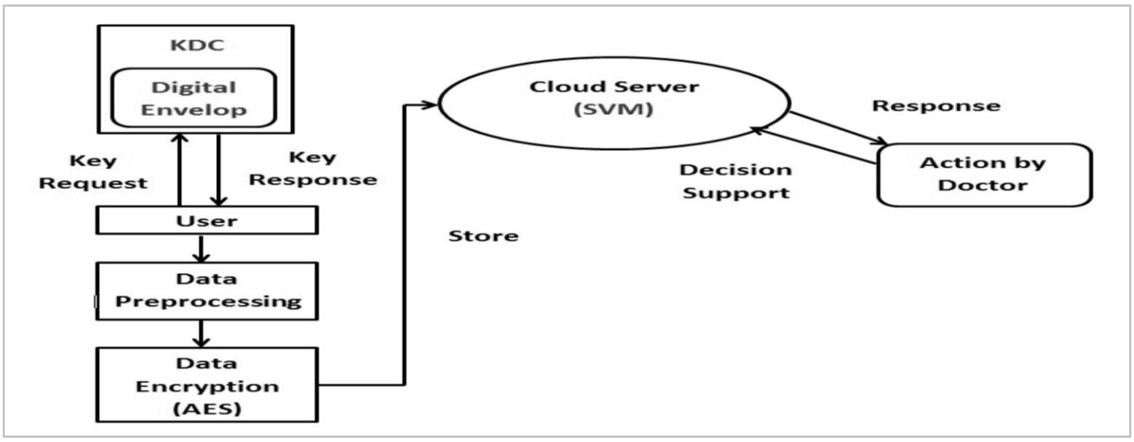

Fig 1. System Architecture

METHODOLOGY

The proposed MSS system consists of seven layers: data collecting, data aggregation, cloud processing, action, AES encryption, KDC, and Digital Envelope. The data collection layer collects data from patients or medical laboratories (users) utilising medical instruments, BBNs, or data storage for on-demand access by healthcare experts. KDC is a facility that has the power to distribute keys to authorised users. In this case, the user requests a key from KDC, and KDC responds by sending the key to the server. The digital envelope approach is employed to improve security. Here, the KDC generates the keys again, requiring two keys for encryption and decryption. The most significant building component is data aggregation or preprocessing data, which generates a training file of acquired data in the data collection layer. And then transmitting the resulting data to the cloud. The most significant function of the cloud is safe storage, which is required for accurate diagnosis and long-term patient health monitoring data. Using sophisticated homomorphic encryption techniques, privacy-preserving computation in the cloud is possible. AES Encryption is used to encrypt and decode data, as well as give protection against attackers and data tampering. The cloud's third role is data analytics, which allows healthcare practitioners to make better decisions using the SVM machine learning algorithm. The action layer Healthcare professionals can be send encryption testing file on cloud. Healthcare professionals have taken right decision on training and testing file by using SVM classifier, which is generate the prediction and sending its predictions in encrypted format.

RESULTS

Comparisons of Proposed System with Existing System

The comparative study based on the domain has a much better performance in terms of both time and memory with respect to the existing systems. Also the key feature being the context which provides the digital envelop to the key generated for encrypted file. The comparative analysis is based on the measures time and memory.

Table 1. Performance analysis of propose system and previous system using time

Sr.No	System		Time in ms
1	Previous system	Without KDC	2000 ms
2	Proposed system	With KDC	1500 ms

Table 2**.** Memory Comparison

Sr.No	System		Memory in KB
1	Previous System	Without KDC	3000 kb
2	Proposed System	With KDC	2500

CONCLUSION

The MSS framework assists a variety of healthcare providers in making suitable judgments. Because information is kept on cloud servers, security has become a serious problem. With the advent of the cloud computing paradigm, a new form of storage called cloud storage has evolved. Adoption of cloud storage, especially via public or private cloud data storage services, brings with it not just various benefits in terms of dependability, flexibility, and scalability, but also new issues in terms of data privacy, protection, and security. This method uses the AES cryptography and digital envelope concepts to address the issue of security. In addition, the system employs a KDC design to reduce the user's load in terms of key generation. KDC uses a digital envelope in which a symmetric key is encoded using the asymmetric key of each unique user, increasing security. The experimental result provides a comparison graph between the systems with and without the KDC system. According to the findings, systems with KDC consumed less time and memory than systems without KDC. In the future, we will be able to employ any medical hardware equipment to assist us in making decisions. We may also utilise an alternate backup to store the data in order to avoid any data loss issues.

REFERENCES

[1] OvuncKocabas, TolgaSoyata, and Mehmet K. Aktas, “Emerging Security Mechanisms for Medical Cyber Physical Systems”, IEEE/ACM transactions on computational biology andbio-informatics, vol. 13, no. 3, may/june2016.

[2] Phaneendra Kumar, Dr.S.V.A.V.Prasad ,ArvindPatak, “Design and Implementation of MHealthSystem by Using Cloud Computing”, Future Gener. Comput.Syst.,Vol. 5, Issue 5,May 2016.

[3] Tran Viet Xuan Phuong, Guomin Yang, Member, IEEE, and Willy Susilo, Senior Member,IEEE, “Hid-den Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions”,IEEE transactions on information forensics and security, vol. 11, no. 1, January 2016.

[4] Abdelghani Benharref and Mohamed Adel Serhani, “Novel Cloud and SOA-Based Framework forE-Health Monitoring Using Wireless Biosensors”, IEEE journal of biomedical and health informatics, vol. 18, no. 1, January 2014.

[5] OvuncKocabas, TolgaSoyata, “Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing”, 2015 IEEE 8th International Conference on Cloud Computing.

[6] X. Yao, Z. Chen, and Y. Tian, “A lightweight attribute-based encryption scheme for the internet of things”, Future Gener.Comput.Syst., vol. 49, pp. 104-112, 2015.

[7] O. Kocabas and T. Soyata, “Towards privacy-preserving medical cloud computing using homomorphic encryption”, in Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, T. Soyata, Ed. Hershey, PA, USA: IGI Global, 2015, ch. 7, pp. 213-246.

[8] J. A. Akinyele, C. Garman, I. Miers, M.W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, “Charm: A framework for rapidly prototyping crypto systems”,J. Cryptographic Eng., vol.3, no. 2, pp. 111-128, 2013.

[9] Robert Mitchell, Ing-Ray Chen, Member, IEEE, “Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems”, Robert Mitchell, Ing-Ray Chen, Member, IEEE, 2013.

[10] Alhassan Khedr, Member, IEEE, and Glenn Gulak, Senior Member, IEEE, “SecureMed: Secure Medi-cal Computation using GPU-Accelerated Homomorphic Encryption Scheme”,2016.

[11] P. Khan, Y. Khan and S. Kumar, "Tracking and Stabilization of Heart-Rate using Pacemaker with FOF-PID Controller in Secured Medical Cyber-Physical System," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), **2020**, pp. 658-661, doi: 10.1109/COMSNETS48256.2020.9027302.

[12] M. Wankhade and S. V. Kottur, "Security Facets of Cyber Physical System," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), **2020**, pp. 359-363, doi: 10.1109/ICSSIT48917.2020.9214079.

[13] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications," in IEEE Access, vol. 8, pp. 151019-151064, **2020**, doi: 10.1109/ACCESS.2020.3016826.

[14] A. I. Newaz, A. K. Sikder, L. Babun and A. S. Uluagac, "HEKA: A Novel Intrusion Detection System for Attacks to Personal Medical Devices," 2020 IEEE Conference on Communications and Network Security (CNS), **2020**, pp. 1-9, doi: 10.1109/CNS48642.2020.9162311.

[15] Z. Wang, P. Ma, X. Zou, J. Zhang and T. Yang, "Security of Medical Cyber-physical Systems: An Empirical Study on Imaging Devices," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications

Workshops (INFOCOM WKSHPS), **2020**, pp. 997-1002, doi: 10.1109/INFOCOMWKSHPS50562. 2020.9162769.

[16] S. Dziembowski and K. Pietrzak, ―Leakage-resilient cryptography, in Proc. IEEE 49th Annu. IEEE Symp. Found. Comput. Sci., 2008, pp. 293–302

[17] Y. Zhou and D. Feng, ―Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing. IACR Cryptol. ePrint Archive, vol. 2005, p. 388, 2005.

[18] O. Kocabas and T. Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption", in Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, T. Soyata, Ed. Hershey, PA, USA: IGI Global, 2015, ch. 7, pp. 213-246.

[19] Abdelghani Benharref and Mohamed Adel Serhani, "Novel Cloud and SOA-Based Framework forE-Health Monitoring Using Wireless Biosensors", IEEE journal of biomedical and health informatics, vol. 18, no. 1,January 2014.