International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Implementation of Secure Decision Support System in Medical Cyber Physical Network

Jayshree V. Ingle[1], Nitin Chopde[2]

[1]Computer Science and Engineering Department, G. H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India

[2]Assistant Professor, Computer Science and Engineering Department, G. H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India

Article Info
Volume 8, Issue 4
Page Number: 258-265

Publication Issue :
July-August-2021

Article History
Accepted : 20 July 2021
Published: 27 July 2021

ABSTRACT

Medical Secure Systems (MSSs) communicate with one another through the use of computation, much as they do with physical operations. MSS speculations and applications are beset by numerous difficulties. In this paper, the primary purpose is to provide a more notable under-remaining of this emerging multidisciplinary strategy. Medical Secure Systems is the name given to the work system that focuses on the MSS in medical applications and is referred to as such (MSS). Using MSS, numerous types of data can be moved to a private or public cloud for increased capacity and processing efficiency. On top of this data, artificial intelligence calculations can be applied to process the information, which will be valuable in the future when selecting a healthcare master. This information can be sensitive, and it is made available to the public as well as for pariahs to have additional space, with the result that the unpleasant issue of security is becoming more prevalent. In order to provide security, we used cryptographic strategies, such as the AES algorithm, to scramble the data before storing it on cloud servers in this paper. After that, in order to improve security even further, the system will make advantage of the possibility of a digital envelope. In this concept, the data encryption AES key is regulated once more through the use of the ECC encryption key. Again, in order to reduce the administrative burden associated with key administration, the system makes use of the Key Distribution Center (KDC), which is capable of producing and managing keys for all customers. According to the findings of the most recent study, this MSS structure is more secure than the previous one, and it also reduces the amount of time spent on important administration duties. The system also receives less time and memory for the purpose of updating its configuration.

Keywords: Digital Envelope, Medical data privacy, Medical Secure systems, Encryption.

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

I. INTRODUCTION

As of late, the study into Medical Security Systems (MSS) has gained prominence as a result of its widespread visibility in the public eye, economic, and social condition, and it has drawn in a large number of analysts from the academic community, associations, and the government. Medical Secure systems are widely regarded as the next generation of built systems, combining correspondence, calculation, and control to achieve the goals of stability, execution, vigour, and proficiency for Medical Secure systems, as well as for other systems. When MSS is heading towards this point, security considerations are not taken into account at the time. Nowadays, the use of MSS is widespread in numerous critical systems, and a framework compromise might put a substantial amount of information at risk. When a glitch in vehicle-to-vehicle communication occurs, the likelihood of a mishap increases because the distance between vehicles is not precisely evaluated and moved. To be honest, the development of self-governing automobiles has only served to further entrench the issue, as travellers must trust the vehicles' decisions at all times. The unstoppable force that drives the operation of such devices allows for the improvement of a comprehensive patient health monitoring framework that can be used in medical settings. The distributed sensor can collect medical data and transmit it to the general public or to private cloud administrations, depending on the configuration. On the cloud, where a gathering of quantifiable surmising algorithms is in operation, the relationship between the patient data and the illness state can be selected for the purpose of distinguishing the illness state. These connections can be forwarded to a restoration administrations expert for assistance in making a decision. Medical Secure Systems (MSS) are systems like the one described above that signal the beginning of a new era in Digi-tal-Health (D-Health) and a potentially dangerous progress in the history of mankind. When constructing MSSs, it is necessary to resolve a variety of mechanical challenges that arise during the development of the auxiliary sections of MSSs, such as sensors, and the integration of distributed computing structures, as well as the rapid web and mobile cellphones. In addition, 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 Medical Secure System has a seven-layer structure, with the layers being information procurement, information aggregation, cloud management, activity, AES encryption, Key Distribution Center, and Digital Envelope, among other things. The following are some thoughts on the seven layers of the human personality:

- Data security is typically provided via a Body Area Network (BAN), which includes distant sensors for specialised restorative applications, such as pulse and internal heat monitoring, as well as data storage for on-demand access by doctors. A BAN awakens the collection of patient health records and promotes this knowledge to a nearby location via the usage of a computationally proficient device.

- The information collection structure square is the most important structure square of an Internet of Things-based design because it allows individually insignificant gadgets to have substantial overall value by concentrating the data from each gadget and sending the accumulated information to the cloud.

- In order to provide precise assurance, long-term patient well-being monitoring information is required. The cloud's secure limit is the most significant capacity available. Handling protection-preserving operations in an open cloud can be accomplished with relative ease by utilising modern homomorphic encryption plans. The third capability of the cloud is data inspection, which can be used to invigorate choice assistance for medical services professionals. The movement provided by the activity layer might be either dynamic or uninvolved. The usage of an actuator is common in dynamic activities because it allows the results of calculations that are still running in a cloud to be converted into the initiation of an actuator. During latent activity, no physical movement is actually taken place.

- AES Encryption is used to encrypt and decrypt data, as well as to protect it from being stolen or altered by an attacker or in-formation correction.

- A Key Distribution Center (KDC) is a facility that has the authority to distribute keys to clients that have been validated. Clients submit a key request to KDC, and KDC responds by providing the key to the server as a response.

- The digital envelope plan is used to increase the security level; in this case, the key distribution center (KDC) creates the keys infers for encryption and unscrambling, which requires two keys from the client.

In this paper, we discuss the related work that has been completed in Section II, the proposed approach modular description, mathematical modelling, algorithm, and experimental setup in Section III, and the future directions for this work in Section IV. Finally, in Section IV, we present a summary of our findings.

II. RELATED WORK

This section discusses the writing audit in insight concerning the medical secure framework.

According to Creators [1], the overall design of an MPCS consists of four layers: data security, data aggregation, cloud handling, and activity management. The hardware and correspondence constraints of each tier differ, but unmistakable encryption plans must be employed to ensure that the data secured within that layer is not compromised outside of that layer. This assessment brings together traditional and emerging encryption systems, taking into account their ability to provide guaranteed storage, data sharing, and secure estimation. In order to successfully execute MCPSs, it would be necessary to overcome creative roadblocks in the development of the auxilia-ry components of the MCPS, such as sensors, distributed computing structures, and fast Internet and mobile phone connections. It will also be necessary to design a sophisticated encryption structure for an MCPS in order to ensure that personal health records are not compromised at any stage during their transmission from mobile phone associations and from the cloud to experts' mobile devices. While this plan recommends only secure hoarding and the use of typical encryption plans, constructing encryption plans opens the door to new possibilities for secure information sharing and secure calculation. The promise in this paper is two-fold: first, it states that the first step in this audit was to apply common practises and create encryption with the goal of implementing MCPS. Second, by providing secure capacity, secure data sharing, and safe computation, these plans provide a comprehensive evaluation and distinguish them from one another in terms of their ability.

Kumar and colleagues [2] are working on the implementation of a medical services architecture that will be based on distributed computing. It will

prepare the structure for the delivery of EMR, for example, Electronic Medical Records of patients, which will be extremely valuable for patient explanation and quick change preparation, as well as for therapeutic sharpening authorities who require in-terminable restorative cases for their own re-see reason. As soon as the patient's essential parameters exceed the specified threshold, this system will alert the user and provide a planned response.

It was proposed in the study [3] to develop two new figure content approach characteristic based encryption (CP-ABE) plots, in which they achieve their goal and are depicted by an AND-door with an additional trump card. They begin with the arrangement and then move on to another methodology that addresses quality with only a single total component, whereas existing ABE plans of an identical sort must employ three distinct accumulation sections to treat a characteristic for each of the three conceivable qualities. Their new methodology leads in a completely new CP-ABE conspire with constant figure content size, which, despite the fact that it can't conceal the entrance approach utilised for encryption, is nevertheless ineffective. Essentially, the purpose of this work is to present an additional CP-ABE contrivance with the forces signals of concealed get admission to the course of action by way of approach for improving the procedure that is now in use inside the age of our in any case plan. Particularly, demonstrate how to join ABE by relying just on AND-door with bargaining chip with inner item encryption, and then utilising the latter to obtain the cause for a hidden access configuration.

Benharref and colleagues [4] suggest a framework that may be used to collect data continually, undertake adequate non-intrusive checking, and propose corrective or potentially lifestyle commitment at whichever moment is necessary and appropriate. A stable consolidation of many innovations, applications, and organisations is made possible by the structure, which is based on organisation oriented planning (SOA) and the Cloud. The adaptable improvement makes it possible to quickly acquire and provide fundamental assurances from a patient's wearable biosensors while taking into consideration the phone's obligated restrictions and force drainage, as well as spasmodic framework partitions. As a result of SOA, data is stored in the cloud and made accessible to specialists, paramedics, and other authorized individuals. It is demonstrated in this study that a revolutionary electronic social insurance system, named the Service-Oriented and Cloud-Based e-Wellbeing Framework, may be developed (SOCBeS).

When everything is said and done, the research presents a methodology [5] that alleviates information security concerns in a social cloud environment by applying a newly developed encryption procedure known as completely Homomorphic Encryption, which is still in its early stages (FHE).

FHE's ability to provide estimations without requiring a thorough examination of the data itself makes it a compelling selection for some restorative applications. When it comes to our possibility evaluation, they employ cardiovascular wellbeing monitoring. They also provide the inclinations and challenges of our technique through the usage of an FHE library that is already installed on the computer system called HElib. Distributed computing has the potential to lower social insurance costs by increasing capacity and processing power.

In order to address the security and protection concerns associated with the Internet of Things, a lightweight no-matching ABE plot based on elliptic bend cryptography (ECC) is suggested [6]. The suggested plot's security is dependent on the ECDDH assumption, despite the fact that it is based on the bilinear Diffie-Hellman assumption, as proved in the quality-based specific set model. The balance

investigations using the major ABE plans are carried out in depth by looking at the rules in a consistent manner and identifying the metrics for calculating the correspondence overhead and computational overhead.

It is possible to use a story-restorative dispersed figuring technique that does not rely on the cloud provider and so avoids security concerns. Our approach makes use of completely homomorphic encryption (FHE), which allows computations to be performed on individual health information without the need to inspect the underlying data when in doubt. For the purpose of demonstrating attainability, we demonstrate the use of a running application for long-distance cardiovascular wellness monitoring that makes use of a pre-installed open-source FHE library [7]. De-recorders is a developer who is primarily concerned with the programming development technique for cryptographic systems [8]. The structure was designed and built in order to reduce the amount of information available to cryptographers. Low-level numerical code, which is frequently a bottleneck during exhibitions, is written in C and is called from the significant-level Python code, which is written in Python. Designs are created in Python, with designers appreciating the marketing advantages of the inherent features of that substantial level language, as well as the structural Toolbox and other mechanisms provided by Charm.

Appeal includes a convention motor that handles with the interchanges, serialisation, and other housekeeping tasks that are essential to the implementation of a multi-party convention in its various forms [9]. Engineers are sheltered from the minutia that isn't associated with the cryptographic theory that has been established in their organisation in this way [10].

III. IMPLEMENTATION DETAILS

This section discusses the system overview in detail, proposed algorithm, and mathematical model of the proposed system.

3.1 System Overview

Detailed descriptions of the proposed system are as follows:

- Browse Dataset

User browse the input dataset, this dataset is depend on medical dataset of patients. Details about the dataset were discussed in the next sections.

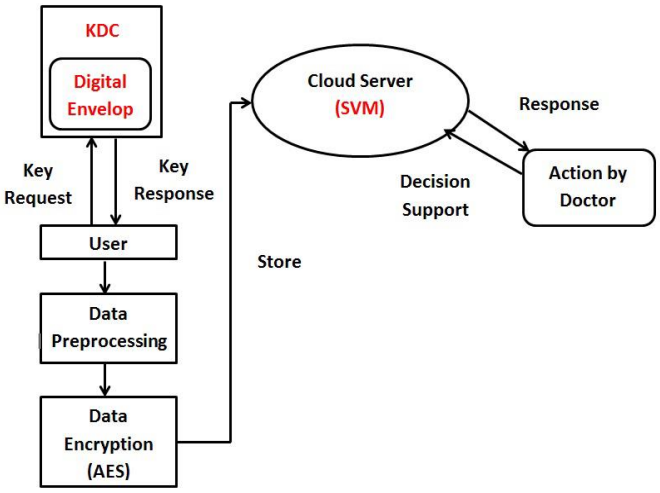

Fig. 1. System Architecture

- Data Preprocessing

In data preprocessing of dataset is done. Firstly dataset is read and produce the training file for the classification process.

- Data Encryption

Due to the security purpose the system encode the data by using the AES Algorithm. Steps of AES algorithm and working of AES algorithm discuss in the algorithm sections.

- Classification

Classification execute the operation of decision support system, for recognizing the patient data. Initially doctor send the request to the server for identifying the health data, at server side SVM

classifier perform the classification process and give the results to the doctor, doctor get data and decrypt the data.

- Key Distribution Center (KDC)

This plan includes KDC and TPA which execute Digital encompass and respectability checking individually. Right off the bat, framework login to cloud server and mention to KDC for the key. KDC will create an ace key and pair of open key and mystery key by utilizing AES and ECC calculation. At that point KDC encodes the ace key utilizing ECCs open key of the mentioned information proprietor and sends the scrambled ace key and mystery key to information proprietor. Subsequent to getting key, information proprietor section the record into squares, encode them utilizing a scrambled ace key, and send to the cloud server.

3.2 Algorithm

Algorithm 1: Digital Envelope

1) Get user request Ui for key generation.
2) Run algorithm 1 (AES key generation)
Get Master key MK
3) Run algorithm 2(ECC key generation)
Get key pairs (PK, SK)
4) Encrypt MK using PK
Get encrypted MK as PK
5) Send PK and SK to requested User Ui

Algorithm 2: AES Algorithm

Input: Plaintext Block ptxtb,
Secret key sk
Output: AES state state
Process:
State = InitState(ptxtb, sk)
AddKey(state, sk0)
For i = 1 to nr-1 do
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddKey(state, keyi)
SubBytes(state)
ShiftRows(state)
AddKey(state, keynr-1)

IV. RESULTS AND DISCUSSION

4.1 Dataset Used

For this system we have taken medical health dataset as a input data for developed the system.

4.2 Results

In this section discussed the experimental result of the proposed system. In table 1 shows the time taken for the proposed system as well as existing system. The accompanying table describes that the time required for executing the framework with KDC is not accurate the time required for executing the framework without KDC.

Table 1. Time Consumption

System	Time in ms
Without KDC	2000 ms
With KDC	1500 ms

Following figure 2 displays the time comparison graph of the proposed system with the existing system. Comparison graph shows that the time required for implementing the system with KDC is less than the time required for implementing the system without KDC.

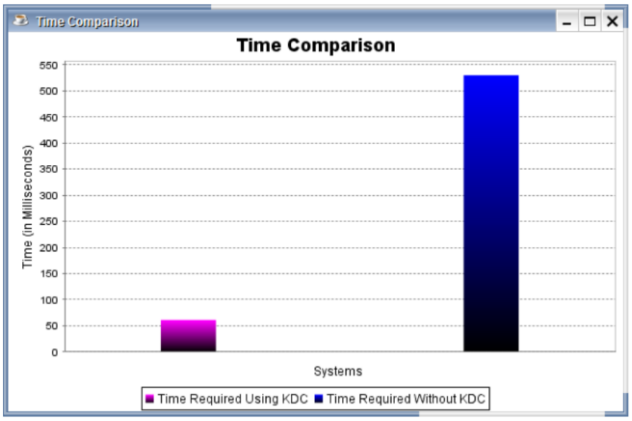

Fig. 2. Time Comparison

In table 2 shows the memory required by the proposed system and existing system. The following table shows that the memory consumed by system without KDC is more than the system with KDC.

Table 2. Memory Comparison

System	Memory in KB
Without KDC	3000 kb
With KDC	2500 kb

Following figure 2 shows the memory comparison graph of the proposed system with the existing system. Following comparison graph shows that the memory utilized by system without KDC is more than the system with KDC.

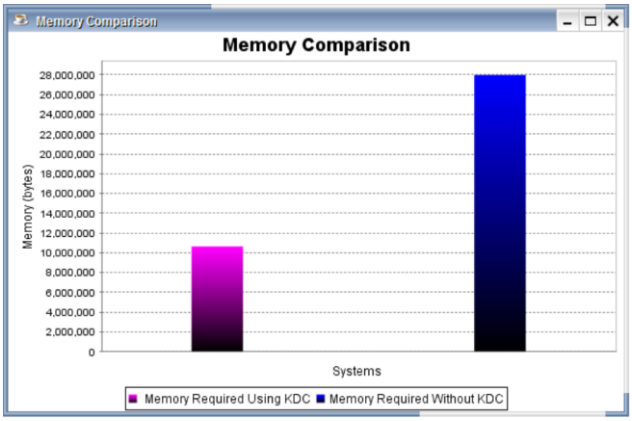

Fig. 3. Memory Comparison

V. CONCLUSION

This system the MSS supporting various medicinal services experts to make proper choices. The security becomes significant concern issues due to the Information is saved money on cloud servers. This framework tackles the issue of security by using the possibility of AES cryptographic and computerized envelope idea. Additionally, the framework utilizes KDC design to diminish the weight of the client as far as producing keys. KDC executes advanced envelope in which symmetric key is encoded utilizing in-dividual clients deviated key which builds the security. The exploratory outcome shows a correlation diagram among the framework by utilizing the KDC framework just as with-out utilizing the KDC framework. From the results it was concluded that framework with KDC required less time and memory than the framework without KDC. In the future, we can utilize any medical equipment gadgets to take choice sup-port. Likewise, we can utilize elective reinforcement to store the information to forestall any information misfortune issues.

VI. REFERENCES

[1]. OvuncKocabas, TolgaSoyata, and Mehmet K. Aktas, “Emerging Security Mechanisms forMedical 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, “Hidden 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 Medical Computation using GPU-Accelerated Homomorphic Encryption Scheme",2016.

Cite this article as :

Jayshree V. Ingle, Nitin Chopde, "Implementation of Secure Decision Support System in Medical Cyber Physical Network", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 4, pp. 258-265, July-August 2021.

Journal URL : https://ijsrset.com/IJSRSET2183215