International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : 10.32628/CSEIT19537

Secure Decision Support System in Medical Cyber Physical Network

[1]Devshri Kothekar, [2]Prof. Pragati Patil

[1]PG Scholar, Department of Computer Science Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India.

[2]Assistant Professor, Department of Computer Science Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India.

ABSTRACT

Medical Secure Systems (MSSs) are represented by integrating calculation as well as physical processes. The speculations and utilizations of MSSs face the large problems. The main objective of this work is to provide a greater understanding of this emerging multidisciplinary methods. In this work system focusing on the MSS in medical applications, which is called as Medical Secure Systems (MSS). In MSS, different types on data can transfer to the private or public cloud for storage and processing. Over this information, machine learning algorithms can be combined to process that data, which will be further helpful to take a few decisions for healthcare expert. This information can be sensitive and is publically accessible and gave to outsider storage space, so that the difficult problem of security is emerges. To providing the security, in this paper we applied cryptographic method, for example, AES to encrypt the data before store on cloud servers. After this, to enhance the further security, system will utilize the idea of digital envelope. In this concept, information encryption AES key is again determined by utilizing ECC encryption key. Again to reduce the key management overhead, framework makes utilization of Key Distribution center (KDC), which can generate and deal with the keys for all users. At the last experimental results presented that, this MSS framework is more secure than existing one and it is additionally reduces the key management overhead. Also system gets less time and memory for implementing the system.

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

I. INTRODUCTION

Recently, the analysis in area of Medical Secure systems (MSS) has become popular because of its wide reflection in society, economy, and environment and has attracted various researchers from academia, organization also from government. Medical Secure systems are generally taken as new generation of engineered systems having the combination of communication, computation and control for achieving the goal of stability, performance, robustness, and efficiency for Medical Secure systems. At time of moving towards this aim security consideration in MSS is neglected. Now a day's, use of MSS are extensively used in numerous vital systems in such cases a system hack can create a major risks. For example, a hack in vehicle-o- vehicle communication is happen, there can be a chances of accidents when distance is not measured and transferred correctly. In fact, the development of autonomous cars has additionally disintegrated the problem since passengers need to trust all choices made by the vehicles. The force which is cannot be stopped in implementation of devices like this enables the development of complete patient health monitoring system which can be used medically. The

distributed sensor can gather the medical information and forwards it to the public or private cloud services. On the cloud where a group of statistical inference algorithm is performing may decide the correlation of the patient information for identifying the diseases state. These correlations can be forwarded to the medicinal services professional for decision support. Systems like above known as Medical Secure Systems (MSS), sign of the start of a novel Digital- Health (D-Health) time and a problematic innovation in human history. While developing MSSs there is a need of solving many issues related to mechanics while generating the structural segments of MSS such as sensors and merging the cloud computing structures also speedy internet with the mobile phones. Also giving the security of personas health information which is transmitted to cloud with help of sensory networks and from cloud to the medical expertise cell phones will need the refined cryptographic engineering methods for MSS. While this arrangement suggest just secure storage using ordinary encryption plans, encryption techniques, rising encryption techniques offer alternatives to protect data sharing and secure calculation. In this structure Medical Secure System as a Seven-layer structure which are information acquisition, data aggregation, cloud processing, action, AES encryption, KDC and Digital Envelope layers. Detail about the seven layers is as follows:

- Data acquisition layer is ordinarily a Body Area Network (BAN) including remote wireless sensors for particular medicinal applications, for example, blood pressure and body temperature observing, or information storage for on request access by doctors. A BAN inspire the collection of patient medical data and advances this data to a close-by computationally capable device.
- A data aggregation is the most important building block of an IoT based engineering, since it allow individually powerless devices to have strong overall usefulness by concentrating the information from every device and sending the aggregated data to the cloud.
- For accurate determination requires long term patient health observing data, secure capacity is the most important function of the cloud. Privacy preserving processing in a public cloud is just achievable utilizing progressed homomorphic encryption plans. Third function of the cloud is information insepection to encourage decision support for healthcare experts. The action layer can give either active or passive activity. In active actions, an actuator is utilized to turn the results of the algorithms that keep running in the cloud into the initiation of an actuator. In passive action, no physical move is really made.
- AES Encryption is exploited to encode and decode the information and provide the security from attacker or data modification.
- KDC is a Key Distribution Center whose have authority to conveyed keys to the authenticated users. Here users sends the request to KDC for key and KDC give key to the server as a response.
- Digital envelope plan is utilized to enhance the security level, here KDC again generate the keys implies for encryption and decryption user require two keys.

In this paper we study about the related work done, in section II, the proposed approach modules description, mathematical modeling, algorithm and experimental setup in section III .and at final we provide a conclusion in section IV.

II. RELATED WORK

In this section discuss the literature review in detail about the medical secure system.

Authors[1] implies that the general architecture of an MPCS include 4 layers: Data acquisition, Data aggregation, Cloud processing, and action. While contrasts in equipment and correspondence capacities

of every layer, distinctive encryption plans must be utilized to make sure that the information protected inside that layer. This review incorporates ordinary and rising encryption plans in light of their capability to give protected storage, information sharing, and secure estimation. Executing MCPSs would require conquering innovative obstacles in building the structural segments of the MCPS such as sensors, cloud computing architectures, and quick Internet and cellular phone connections. Additionally, guaranteeing the protection of the individual health records sooner or later of the transmission from cellular phone connections and from the cloud to doctors cellular devices will require the design of an advanced cryptography structure for a MCPS. While this design implies only secure storage the use of traditional encryption schemes, emerging encryption schemes gives options for secure data sharing and secure computation. In this paper the contribution is two-overlap: First of all this review utilized ordinary and developing encryption plans to actualizing MCPS. Secondly this plans give broad assessment and contrast them in light of their capacity with give secure capacity, secure information sharing, and secure calculation.

Kumar et al. [2] are implementing a health care system which will be coordinated with cloud computing. It will make framework equipped for producing EMR i.e. Electronic Medical Records of patients which will be highly valuable for patient's analytic and fast change prepare and in addition for medicinal honing specialists who require endless medicinal cases for their own review reason. This framework will monitor patient's health in a suitable way and produce ready when the patient's fundamental parameters crosses the ordinary esteem.
The paper [3] developed two new cipher text policy attribute based encryption (CP-ABE) plots in which the get to arrangement is characterized by AND-gate with wild card. begin with the plan, they initiate another approach that utilization just a single aggregate component to speak to a attribute, while the current ABE plans of a similar sort need to utilize three distinctive gather components to speak to an attribute for the three conceivable values. Their new approach outcomes in a brand new CP-ABE scheme with constant cipher text size, which, however, cannot hide the access policy used for encryption. The essential commitment of this paper is to propose another CP-ABE conspire with the possessions of covered up get admission to arrangement by way of amplifying the technique this utilized inside the generation of our to begin with plan. Particularly, show a manner to bridge ABE primarily depend on AND-gate with wild card with internal product encryption after which use the latter to acquire the purpose of hidden access policy.

Benharref et al. propose [4] system used to collect patients information progressively, perform suitable non meddling checking, and propose restorative or potentially way of life engagements, at whatever point required and suitable. The structure, which is predicated on administration orientated design (SOA) and the Cloud, permit a consistent incorporation of various innovations, application and administrations. It moreover coordinate with versatile improvement to effortlessly collect and impart imperative certainties from a patient's wearable biosensors even as pondering the cell phones constrained capacities and power seepage likewise to discontinuous system separations. At that point information are put away inside the cloud and amp; made accessible through SOA to permit simple access by doctors, paramedics, or some other approved element. This paper displays a novel electronic social insurance framework, called Service Oriented and Cloud-Based e-health Framework (SOCBeS).

The paper present an approach [5] that depart information protection worries in general society cloud situation, by method for using a rising encryption procedure called completely

Homomorphic Encryption(FHE).FHE can permit calculations without really watching the information itself makes it an appealing choice for certain therapeutic applications. In this paper, they utilize cardiac health observing for our possibility evaluation and provide the preferences and difficulties of our approach by using an entrenched FHE library called HElib. Cloud computing can decreases healthcare costs by expanding the storage and computation.

To solve the security and privacy problems in IoT ,a lightweight no-pairing ABE scheme depend on elliptic curve cryptography (ECC) is proposed. The security of the proposed scheme is based on the ECDDH assumption in spite of bilinear Diffie-Hellman assumption, and is proved in the attribute based selective-set model. By uniformly examining the criteria and defining the metrics for measuring the communication overhead and computational overhead, the contrast analyses with the prevailing ABE schemes are made in detail.

A novel medicinal distributed computing method that dispenses with security concerns connected with the cloud supplier. Our technique utilize completely Homomorphic Encryption (FHE),which allows calculations on individual health data without as a general rule watching the basic information. For an achievability consider, we exhibit a running usage of a long haul cardiovascular health observing application the utilization of an entrenched open source FHE library [7]. Describes a programmer concentrated on software development methodology for cryptographic systems[8].To reduce the load on cryptographer authors designed and construct the framework. Low-level mathematical code, often a performance bottleneck, is written in C, and is called from the high level Python code. Developers constructs their protocols in Python and enjoy the advantages of the built in features of that high level language, and the framework Toolbox and other mechanisms offered by Charm. Charm contains a protocol engine that takes care of the communications, serialization and other house-keeping that is integral to implementing a multi-party protocol. Thus, developers are protected from the minutia that is not related to the cryptographic theory in their protocol.

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.

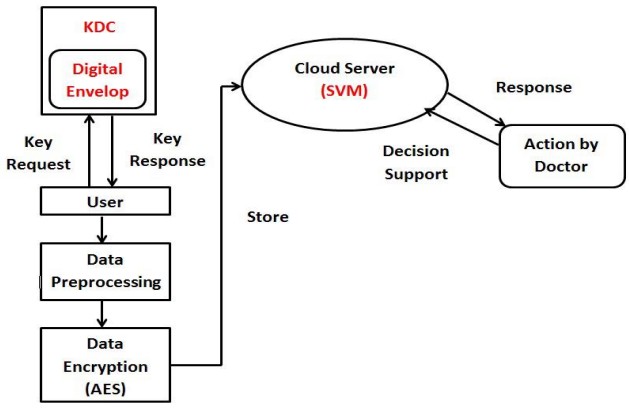

Fig. 1. System Architecture

- 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 scheme involve KDC and TPA which execute Digital envelop and integrity checking respectively. Firstly, system login to cloud server and requesting to KDC for key. KDC will produce master key and pair of public key and secret key by using AES and ECC algorithm. Then KDC encode the master key using ECCs public key of requested data owner and send the encrypted master key and secret key to data owner. After getting key, data owner fragment the file into blocks, encrypt them using encrypted master 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)

3.3 Mathematical Model

Let S be a decision support system for healthcare professionals.
S is consist in following way,
S = {Input, Process, Output}

Input
Browse Dataset
U= {u1, u2, u3,...,un}
Where, U is a set of number of related papers and u1, u2,
u3,....,un are the number of papers.
Process D = Dataset
Get input dataset
Dataset D = HEART DISEASES Dataset

HEART DISEASES Dataset obtain from Cleveland database.
Cleveland dataset concerns classification of person into normal and abnormal person regarding heart diseases.

Process
1) User Registration and login
U = {u1, u2,....., un}
Where, U is the n number of registered users on cloud server.
User should be successfully registered and logged into the system, to access all facilities provided by users.

2) Key generation and distribution
At KDC,

$$K = \{k1, k2,.....,kn\}$$

Where, K is the set of keys generated at KDC for all requested users.

This AES keys are used to encrypt the data before storing on cloud server.

To reduce the key management overhead, System uses KDC. KDC generate, distribute and manage the keys among multiple users.

Digital Envelope,

D = {d1, d2,.....,dn},

Where, D is the set of digital envelopes of all individual users.

3) At User, Data Preprocessing and Data encryption

In this step, user preprocesses all data to remove stop words and noisy data. After this, to improve the security of data, data encryption technique is applied to encrypt the data for security purpose.

This data is encrypted with AES encryption key received from KDC in digital envelope.

ED = {ed1, ed2,.....,edn},

Where, ED is the encrypted data of n number of users

4) Upload encrypted data

UED = {ued1, ued2,.....,uedn}

Where, UED is the n number of encrypted data which is uploaded on cloud server by n number of users.

5) At cloud server, Data classification

By using SVM algorithm, all received encrypted data is classified. This is useful to well categorize the available data on cloud server.

C = {c1, c2,.....,cn}

Where, C is the set of classified data in n category. It improves the user search experience.

6) Decision Support request from healthcare professionals

R = {r1, r2,.....,rn}

Where, R is the set of n number of requests from n number of healthcare professionals, to take some important decision.

In return professionals received relevant data from cloud server.

Output:

Response to healthcare professionals from cloud server, which is used to take proper decisions.

RSP ={rs1, rs2,.....,rsn}

Where, RSP is the n number of responses provided to healthcare professionals for requested search query.

3.4 Experimental Setup

The system is built using Java framework on Windows platform. The development tool used as a Net beans IDE. The system doesn't require any special hardware to run; any standard machine is able to run the application.

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 Consuption

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.

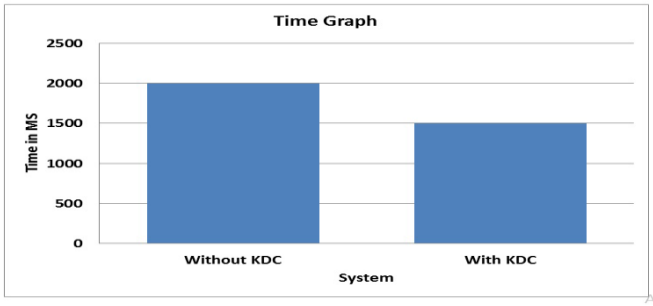

Fig. 2. Time Comparison

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.

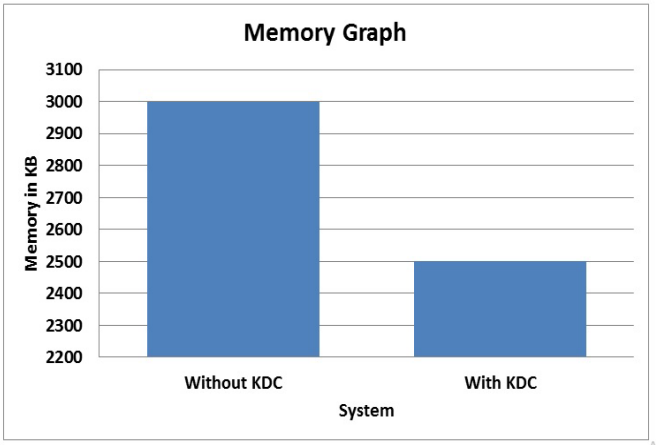

Fig. 3. Memory Comparison

V. CONCLUSION

This framework the MSS supporting to numerous healthcare professionals to take appropriate decisions. The security becomes major concern issues because of the Information is saved on cloud servers. This system tackle the problem of security by utilizing the idea of AES cryptographic and digital envelope concept. Also system uses KDC architecture to decrease the burden of user in terms of generating keys. KDC execute digital envelope in which symmetric key is encoded using individual users asymmetric key which increases the security. Experimental result shows comparison graph among the system by using KDC system as well as without using KDC system. From the outcomes it was conclude that system with KDC required less time and memory than the system without KDC. In future we can use any medical hardware device to take decision support. Also we can use alternative backup to store the data to prevent any data loss problems.

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 :

Devshri Kothekar, Prof. Pragati Patil, "Secure Decision Support System in Medical Cyber Physical Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 1261-1268, March-April 2019.

Journal URL : http://ijsrcseit.com/CSEIT19537