International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Survey on Security Issues in Decision Support System of Health Care 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 2
Page Number : 676-684

Publication Issue
March-April-2021

Article History
Accepted : 05 April 2021
Published : 10 April 2021

ABSTRACT

Medical Secure Systems (MSSs) are spoken to by incorporating count and also physical procedures. The theories and uses of MSSs confront the huge issues. The main objective of this study is to give a more prominent comprehension summary of this developing techniques focusing on the security of the outsourced medical data. In this system, the main focus is on secure data transmission of medical data. Such system is called as Medical Secure Systems (MSS). It can transmit and process the data gathered from health observing systems, which comprises of BAN. The obtained data is transmitted to the private or open cloud which contains a set of calculations for investigating the patient data. These medical data oughts to be kept the mystery. In the wake of breaking down these data, the input is given to the specialists to make a remedial move. This system incorporates data obtaining which is fit for gaining data from body territory systems, data conglomeration which focuses the accumulated flag data, cloud preparing which incorporates numerous examination calculations and activity layer which create either physical activity or choice help. In this paper, we will talk about different issues that should be considered to satisfying the security and privacy necessities and furthermore examine about the important components and wordings utilized by the different specialists to illuminate those issues.

Keywords : Medical Cyber Physical Systems, Secure Digital Cover, Confidentiality, Homomorphic Encryption

I. INTRODUCTION

Recently, researchers are more inclined towards the study in the area of Medical Cyber Physical Systems (MCPS). As it turned out to be famous in light of its wide appearance in the public eye, economy, and condition and has pulled in different analysts from the scholarly community, association additionally from the government. It incorporates the physical parts known as cameras, sensors with cloud and

persistently screens the adjustments in the physical condition. As indicated by WHO report, coronary illness and heart stroke is the prime reason for death. These kinds of death count will reach up to 23.3 million by 2030. To offer regard for these issues, CPS is joined with the Healthcare field. In this way, CPS in Healthcare is regularly alluded to as Medical Cyber-Physical System or Medical Secure systems (MSS).

In this, Sensors is installed in, close by the patient's body to quantify patient's physiological essential signs, for example, temperature, circulatory strain, pulse, breath rate, ECG, EEG, and so forth., If these touchy data are hindered could prompt a few outcomes like mental unsteadiness, relationship issues, even occupation misfortune and wrong medications prompts tolerant demise. Because of this, more consideration ought to be given and taken to give security and privacy to the data. Also, guaranteeing the confidentiality and security of the individual medical data the sharing between the tactile systems to the cloud and from the cloud to specialists' cell phones will require the improvement of a modern cryptographic development for an MSS. While this structure suggests just secure capacity utilizing regular encryption plans, rising encryption plans gives a better substitution for performing secure data sharing and computation. This study discusses about condensing the difficulties identified with cloud and healthcare.

II. REVIEW OF LITERATURE

Here in this part of the discussion we examine the literature survey in insight regarding the secure medical data outsourcing.

Here in this research [1] the author present the structure of an MCPS. This system consist of 4 main layers which are, Data procurement, Data accumulation, Cloud preparing, and activity. It also differentiates in gear and the limits of each layer, a proper encryption design must be used to ensure that the data ensured in that layer. In the present survey author consolidates common and methods for encryption considering its ability to give ensured capacity, data sharing, and secure estimation. Executing MCPSs would require vanquishing inventive snags in building the basic fragments of the MCPS, for example, sensors, distributed computing designs, and fast Internet and phone associations. Furthermore, ensuring the assurance of the individual health records at some point or another of the transmission from PDA associations and from the cloud to specialist's cell gadgets will require the plan of a propelled cryptography structure for an MCPS. While this structure suggests just secure capacity the utilization of customary encryption plans, rising encryption plans gives alternatives for secure data sharing and secure calculation. In this paper the commitment is two-cover: First of this audit used common and creating encryption intends to complete MCPS. Besides these, the presented designs give expansive appraisal and difference them in light of their ability to give a secure limit, secure data sharing, and secure estimation.

Healthcare turns into a major issue because of the absence of accessibility of master specialists. Because of this issue, there is a change in perspective from need-based health checking to preventive health observing administration. Keeping in view this situation author in this paper [2] proposed a health care system which will be coordinated with distributed computing. That will make the system fit for creating EMR, for example, Electronic Medical Records of patients which will assume a valuable job for patient's analytic and quick enhancement process just as for medical rehearsing specialists who require vast medical cases for their very own examination reason. This system will monitor a patient's health in an opportune way and create a ready when the patient's indispensable parameters cross the typical

esteem. The significant data will be exchanged to the distributed storage that can be gotten to by enlisted master specialists and patients by means of the Android App.

This study [3] presented a novel content approach attribute-based encryption (CP-ABE) methods. In CP-ABE logical AND is used to present the plan with a special case. Start with the arrangement, they start another methodology that uses address an attribute by solitary total part. Also the current designs of a system need to use three assemble segments for the three possible qualities by addressing an attribute. The presented methodology in this study results in a fresh out of the plastic new CP-ABE plot with steady figure content size, which, in any case, can't shroud the entrance arrangement utilized for encryption. The main aim of this study is the demonstration of another CP-ABE contrive with concealed to get added to game plan by a method for enhancing the strategy this used inside the age of our in any case plan. Especially, demonstrate a way to connect ABE essentially rely upon AND with trump card with interior item encryption after which utilize the last to get the motivation behind concealed access approach.

Xin Sun [4] et al present a view on the structure of a novel hybrid system for recognizing peculiar traffic in huge scale and strategy rich data systems. This methodology joins static setup investigation and dynamic traffic examination. At first build up the deliberations and scientific models to appropriately display the system and security arrangements to statically check for infringement of system wide invariants, which are potential security vulnerabilities. At that point create dynamic data systematic procedures to examine traffic in real-time and distinguish odd traffic designs that might be abusing the security vulnerabilities. The aftereffects of the static examination will be utilized to help and guide the dynamic traffic investigation to upgrade the asset portion and limit false positives.

In this research author discussed a technique [5] that leave data insurance stresses in general society cloud circumstance, by a technique for utilizing a developing encryption strategy called Fully Homomorphic Encryption (FHE). FHE is capable of performing computations without the complete revelation the data itself settle on it an engaging decision for certain therapeutic applications. The study also uses the cardiovascular health watching for our possibility assessment and give the inclinations and challenges of our methodology by utilizing a dug in FHE library called HElib. Distributed computing can diminish healthcare costs by growing the capacity and calculation.

O. Kocabas [6] endeavors to break down the present examination and improvement on wearable biosensor system for health perceptions. WHMS is vital in the exploration network amid the most recent decade as it is brought up by the various and yearly expanding relating research. As healthcare costs are expanding and the total populace is maturing, there has been a need to screen a patient's health status while he is out of the doctor's facility in his own condition. To address this interest, an assortment of system models and business items have been created throughout ongoing years, which go for giving constant medical data after examination is offered, either to the patient or to a medical center or straight to a directing healthcare experts, while having the capacity to alarm the individual if there is conceivable fast approaching health-compromising conditions. Last few years have seen a developing enthusiasm for portable sensors and today some devices are economically accessible for individual health care, wellness, and movement mindfulness.

T. Soyata [7] proposed a strategy alongside this these systems in health observing utilizations patient's physiological readings and store it in a private or open cloud for a long haul. In the ordinary technique, breaking down a patient's health status, for example,

body temperature ECG etc.is a tedious procedure and may have some blunder factors as well. Be that as it may, on current advancements, for example, remote wearable sensors, it is exceptionally helpful and powerful to investigate patient's health status. In a rush world, it is progressively versatile. Over this procedure, Body Area Network is equipped for catching the flag from the sensors and keep track a record of patient's health status.

At the point when an individual counsels specialist for checking his physical health data, the specialist have the typical lab tests reports, as well as have data that accumulated from the remote wearable sensors. With the assistance of accessible data and data gathered from the system that additionally approach an expansive corpus of perception data for different people, the specialist can improve a much visualization for your health and prescribe treatment, early intercession, and way of life decisions that are especially viable in enhancing the wellness of the body. Such an exceptionally valuable innovation can enhance the field of medical application and ensure and sure about the patient health status. This may summon new musings in the zone of medical science.

There are two enemy models dynamic foe model and latent foe show. The MCPS [8] gives data privacy on dynamic enemy display whereas it gives both privacy and accuracy on inactive for demonstrate. Hotel request to dissect the security needs of the MCPS inactive enemy is broadly utilized.

In distributed computing, the issue related to privacy is based on multi-keyword looking over encoded data. So it requires a set of privacy necessities. It is finished with an effective strategy called —coordinate coordinating. To quantitatively assess such similitude measure. Another strategy utilized is —inner item similitude. To accomplish different stringent privacy prerequisites in two diverse danger models, here first propose a fundamental thought for the MRSE based on secure inward item calculation.

S. Dziembowski proposed encryption components that go through thorough numerical and hypothetical cryptanalysis to give security and privacy, the system may lose data because of the vulnerabilities in its product and equipment usage. Assaults based on such spilled data are called side-channel assaults. These assaults can be averted by utilizing spillage safe cryptography [9]. Looking for countermeasures, one can attempt to avert side-channel assaults by changing the usage or anchoring equipment. This prompts an experimentation approach where usage is made secure against a specific kind of assault just before another progressively successful assault shows up. Spillage Resilient Cryptography receives an alternate perspective by endeavoring to give provably anchor natives within the sight of an extensive variety of side-channel data. Planning measures are spare within the sight of spillage is a troublesome yet not feasible undertaking. The most recent couple of years, the cryptographic network has put a great deal of exertion in developing spillage flexible natives. As the establishments for a hypothetical treatment of the subject have been set, we anticipate that inside the following years increasingly more spillage versatile natives will be developed that will endure more extravagant and more extravagant families F of spillage capacities. Side channel assaults focus on acquiring the mystery/private key by utilizing each layer of the system, instead of simply the data that is being prepared by the system. While numerous kinds of side channel assaults exist for almost every encryption conspire.

Side-channel attacks [10] are emerging because of programming or equipment structure issues. It is anything but difficult to execute against amazing assaults, and their objectives incorporate natives, conventions, modules, and gadgets to even systems. These assaults are causes Sevier issue to cryptographic

segments. To maintain a strategic distance from these issues some cryptographic investigation must be considered. This includes the strategies and systems utilized in these assaults, the damaging impacts of such assaults, the countermeasures against such assaults and assessment of their plausibility and appropriateness; Finally, the most essential end from this paper is that it isn't just a need yet additionally an absolute necessity, in the coming variant of FIPS 140-3 standard, to assess cryptographic modules for their counteractive action towards side channel assaults.

Timing assaults on elliptic bend cryptosystem focus on the scalar augmentation task. It is forestalled by utilizing Montgomery's augmentation strategy which is proposed by P. L. Montgomery [11] plays out the duplication free from the bits of the private key.

This incorporates a calculation for computing elliptic scalar increases on non-excessively particular elliptic bends characterized over GF(2m). The calculation is a little form of technique examined is based on Montgomery's strategy. The calculation is anything but difficult to actualize in both equipment and programming. It works for any elliptic bend over GF (2m), and it requires no pre-processed products of a point and is quicker overall than the expansion subtraction strategy. In an expansion, the strategy requires less memory than projective plans and the measure of calculation required for a scalar increase is settled for all multipliers of a similar double length. Hence, the enhanced strategy has numerous attractive highlights for executing elliptic bends in limited situations. It is a productive strategy for figuring elliptic scalar increases. The strategy performs precisely 6blog2 kc + 10 field augmentation for figuring KP on elliptic bends chose indiscriminately, is anything but difficult to execute in both equipment and programming, requires no pre-calculations, works for any usage of GF(2n), is quicker than the expansion subtraction technique by and large, and utilization less registers than strategies based on projective plans. Thusly, the technique seems helpful for uses of elliptic bends in requirement situations, for example, cell phones, and shrewd cards.

J. Lˇopez proposed a strategy for power examination assaults on AES [12] can be counteracted by utilizing randomized covers for AES activities that scramble the connection between the AES mystery key and the middle of the road esteems produced amid each AES round. Assaults on usage are of specific worry to guarantors and clients of smart cards. Smartcards are turning into a favoured method for safely overseeing applications in businesses, for example, broadcast communications, health care, transportation, pay-TV and web trade. Smartcards have likewise been proposed for use in security applications, for example, organize get to and physical access to areas, for example, cars, homes, and organizations. Smartcards, anyway are conceivably helpless against usage assaults. A smart card microchip has a negligible measure of processing force and memory. Shockingly, programming countermeasures against power examination assaults can result in huge memory and execution time overhead. The measure of overhead appears to rely upon the sort and course of action of the major activities utilized by a calculation. Here it inspects the key activities utilized by every one of the AES finalist calculations. At that point create procedures that utilization irregular veils to make programming executions of these activities impervious to control examination assaults. At long last, utilize these new countermeasures to execute covered renditions of every one of the remaining AES calculations. The execution and usage attributes of these countermeasures in a 32-bit, ARM-based smartcard are broke down.

Power examination based assaults on ECC-based encryption plans can be moderated by techniques recommended that randomize middle of the road calculations to evade data spillage about the private key from power utilization designs.

A ton of consideration has been paid to elliptic bends for cryptographic applications and it has turned out to be progressively regular to actualize open key conventions on elliptic bends over a substantially limited field. Elliptic bends (EC) [13] give a gathering structure, which can be utilized to decipher existing discrete-logarithm cryptosystems into the setting of EC. The executions of elliptic bend crypto-systems, for example, El-Gamal type encryption or Diffie-Hellman key trade are helpless against Differential Power Analysis. Here presented three counter estimates that address explicitly these assaults. Those countermeasures are anything but difficult to actualize and don't affect effectiveness fundamentally. To take care of the issues confidentiality and data security in IoT, a lightweight no-blending ABE method is proposed which is based on a homomorphic encryption mechanism called as Elliptic Curve Cryptography (ECC). The proposed plan assures the safety based on the ECDDH suspicion despite bilinear Diffie-Hellman suspicion, and is demonstrated in the specific set model based on attribute. By consistently looking at the criteria and characterizing the measurements for estimating the correspondence computational load, the balance investigations with the predominant ABE plans are made in detail.

A tale therapeutic circulated processing strategy that sheds security concerns associated with the cloud provider. Our strategy use totally Homomorphic Encryption (FHE), which permits computations on individual health data without when in doubt viewing the fundamental data. For consideration, system exhibits a use of a whole deal heart health watching application [14].

The developer focused on programming improvement technique for cryptograph based systems are presented in this study [15]. To diminish the heap on cryptographer creators planned and build the structure. Machine level code, frequently an execution bottleneck, is written in C and is called from the abnormal state Python code. Engineers build their conventions in Python and appreciate the upsides of the implicit highlights of that abnormal state dialect, and the structure Toolbox and different systems offered by Charm. Appeal contains a convention motor that deals with the correspondences, serialization and other house-keeping that is basic to executing a multi-party convention. Consequently, engineers are shielded from the minutia that isn't identified with the cryptographic hypothesis in their convention.

We did comparative studied on some paper publish on this topic. Here in below table shows previous systems and their disadvantages which are overcome in our system.

Sr. No	Title	Techniques	Advantages	Disadvantages
1.	Emerging Security Mechanisms for Medical Cyber Physical Systems	MCPA System	Their significant Speed-up is necessary either through theoretical advancements or by utilizing GPUs, ASICs, or FPGA-based hardware accelerators.	Low security
2.	A lightweight attribute-based encryption scheme for the internet of things	a lightweight no-pairing ABE scheme based on elliptic curve cryptography	The proposed scheme has improved execution efficiency and low communication costs	Poor Flexibility in Revoking Attribute. Poor Scalability

3.	Towards privacy-preserving medical cloud computing using homomorphic encryption	a novel medical cloud computing approach that eliminates privacy concerns associated with the cloud provider	This study is a good step towards making FHE-based medical cloud computing a reality.	Low security
4.	Charm: A framework for rapidly prototyping cryptosystems	A Framework for Rapidly Prototyping Cryptosystems	Charm is designed to minimize code complexity, promote code re-use, and to automate interoperability, while not compromising on efficiency.	development requirements cannot support Python

III. PROPOSED SYSTEM

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

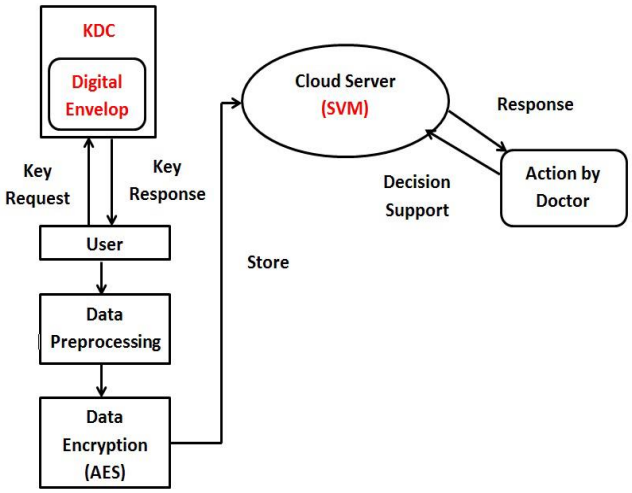

Fig. 1. System Architecture

- 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.

IV. CONCLUSION

In MSS The security winds up significant concern issues in light of the fact that the data outsourced on cloud is the most valuable assets. In this paper we assessed about the different procedures utilized in Medical Cyber Physical Systems, for example, remote body zone systems, cloud, electronic health record, enormous data, web of things and so forth. The security prerequisites of MCPS are likewise examined. Surmising's from the different strategies, required learning about the difficulties and instruments will be valuable to assemble a productive Healthcare System.

V. REFERENCES

[1]. Ovunc Kocabas, Tolga Soyata, 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 ,Arvind Patak, "Design and Implementation of M-Health System 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]. Xin Sun, Fu-Shing Sun, "A Hybrid Approach to Detect Traffic Anomalies in Large-Scale Data Networks", Conference on Computational Science and Computational Intelligence, 2016.

[5]. Ovunc Kocabas, Tolga Soyata, "Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing", 2015 IEEE 8th International Conference on Cloud Computing.

[6]. A. Page, O. Kocabas, T. Soyata, M. K. Aktas, and J. Couderc, —Cloud-based privacy-preserving remote ECG monitoring and surveillance, Ann. Non-invasive Electrocardiol., vol. 20, no. 4, pp. 328–337, 2014.

[7]. M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. K. Aktas, G. Mateos, B. Kantarci, and S. Andreescu, —Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: Opportunities and challenges, in Proc. IEEE Int. Conf. Serv. Comput., Jun. 2015, pp. 285–292.

[8]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, —Privacy-preserving multi-keyword ranked search over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

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

[10]. 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.

[11]. P. L. Montgomery, —Speeding the pollard and elliptic curve methods of factorization, Math. Comput., vol. 48, no. 177, pp. 243–264, 1987.

[12]. J. L opez and R. Dahab, —Fast multiplication on elliptic curves over GF (2m) without pre-computation, in Proc. Cryptographic Hardw. Embedded Syst., 1999, pp. 316–327.

[13]. T. S. Messerges, —Securing the aes finalists against power analysis attacks, in Proc. Fast Softw. Encryption, 2001, pp. 150–164.

[14]. 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.

[15]. 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.

[16]. 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

Cite this article as :

Jayshree V. Ingle, Nitin Chopde, "Survey on Security Issues in Decision Support System of Health Care Network ", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 2, pp. 676-684, March-April 2021. Journal URL : https://ijsrst.com/IJSRST218292