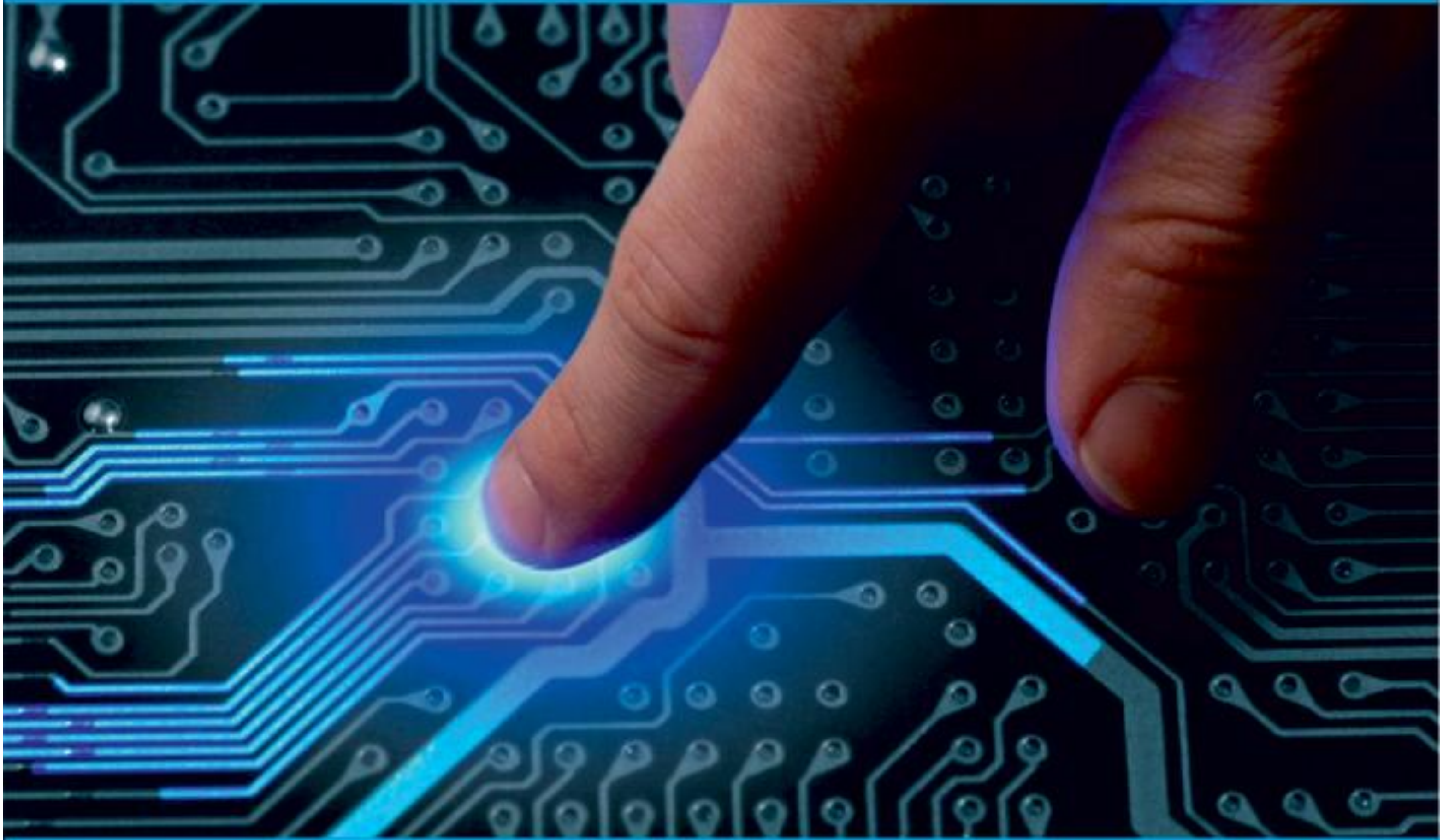
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

IOT Based Emerging Security Frameworks for Medical Cyber Physical Systems

Karan Siwach[1], Miss. Vinita Sharma[2]

M. Tech Student, Department of Computer Science and Engineering, ABSS Institute of Technology, Meerut, AKTU, Lucknow, India [1]

Head of Department, Department of Computer Science and Engineering, ABSS Institute of Technology, Meerut, AKTU, Lucknow, India [2]

ABSTRACT: The following decade will witness a surge in remote health-monitoring systems that are based on body-worn monitoring devices. These Medical Cyber Physical Systems (MCPS) will be capable of transmitting the acquired data to a private or public cloud for storage and processing. Machine learning algorithms running in the cloud and processing this data can provide decision support to healthcare professionals. There is no doubt that the security and privacy of the medical data is one of the most important concerns in designing an MCPS. In this project, we depict the general architecture of an MCPS consisting of four layers: data acquisition, data aggregation, cloud processing, and action. Due to the differences in hardware and communication capabilities of each layer, different encryption schemes must be used to guarantee data privacy within that layer. We survey conventional and emerging encryption schemes based on their ability to provide secure storage, data sharing, and secure computation. Our detailed experimental evaluation of each scheme shows that while the emerging encryption schemes enable exciting new features such as secure sharing and secure computation, they introduce several orders-of-magnitude computational and storage overhead. We conclude our paper by outlining future research directions to improve the usability of the emerging encryption schemes in an MCPS.

KEYWORDS: Medical Cyber Physical Systems, Medical Data Privacy, Homomorphic Encryption, Attribute-Based Encryption

I.INTRODUCTION

Developing MCPSs will needs to avoid the technological hurdles in building the architectural components of the MCPS such as sensors, cloud computing architectures, and fast Internet and cellular phone connections. Additionally, assuring the privacy of the personal health information during the transmission from the sensory networks to the cloud and from the cloud to doctors' mobile devices will necessitate the development of a sophisticated cryptographic construction for an MCPS. While this design implies only secure storage using conventional encryption schemes, emerging encryption schemes provide options for Secure data sharing and secure computation.

The coming decade will witness an explosive growth in systems that monitor a patient through body-worn inexpensive personal monitoring devices that record multiple physiological signals, such as ECG and heart rate[1], or more sophisticated devices that measure physiological markers such as body temperature, skin resistance, gait, posture, and EMG[2]. The emergence of these devices combined with user awareness for their importance in personal health monitoring even emerged trends to make such devices fashionable[3].The unstoppable momentum in the development of such devices enabled the construction of complete patient health monitoring systems that can be clinically used. The medical data that is acquired from patients by a distributed sensor network can be transmitted to private [4], or public cloud services.A set of statistical inference algorithms running in the cloud can determine the correlation of the patient data to known disease states[5]. These correlations could be fed back to healthcare professionals as a means to provide decision support. Such systems, termed Medical Cyber-Physical Systems (MCPS), signal the beginning of a new Digital-Health (D-Health) era and a disruptive technology in human history. Establishing MCPSs will require overcoming technological hurdles in building the architectural components of the MCPS such as sensors, cloud computing architectures, fast Internet and cellular phone connections. Additionally, assuring the privacy of the personal health information during the transmission from the sensory networks to the cloud and from the cloud to doctor’s mobile devices will necessitate the design of a sophisticated cryptographic architecture for a MCPS. While this design implies only secure storage using conventional encryption schemes, emerging encryption schemes provide options for secure data sharing and secure computation.

II.LITERATURE SURVEY

O. Kocabas [1] attempts to analyse the current investigation and development on wearable biosensor system for health observations. WHMS is very important in the research community during the last decade as it is pointed out by the numerous and yearly increasing corresponding research. As healthcare costs are increasing and the world population is ageing, there has been a need to monitor a patient's health status while he is out of the hospital in his personal environment. To address this demand, a variety of system prototypes and commercial products have been produced in the course of recent years, which aim at providing real-time medical information after analysis is given, either to the patient or to a medical centre or straight to a supervising healthcare professionals, while being able to alert the individual if there is possible imminent health threatening conditions.

Recent years have seen a rising interest in wearable sensors and today several devices are commercially available for personal health care, fitness, and activity awareness. T. Soyata [2] proposed a method along with this these systems in health monitoring uses patient's physiological readings and store it in a private or public cloud for long term. In the normal method, analysing a patient's health status such as body temperature ECG etc.is a time consuming process and may have some error factors too.. But on current technologies such as wireless wearable sensors, it is very useful and effective to analyse patient's health status. In a hurry world it is more adaptable. Over this technique Body Area Network is capable of capturing the signal from the sensors and keep track a record of patient's health status.

When a person consults doctor for checking his physical health information, the doctor not only have the normal lab tests reports, but also have information that gathered from the wireless wearable sensors. With the help of available information and data collected from system that also have access to a large corpus of observation data for other individuals, the doctor can make a much better prognosis for your health and recommend treatment, early intervention, and life-style choices that are particularly effective in improving the fitness of body. Such a very useful technology can improve the field of medical application and make sure and confident about the patient health status. This may invoke new thoughts in the area of medical science.

There are two adversary models active adversary model and passive adversary model. The MCPS provides data privacy on active adversary model [3] where as it provide both privacy and correctness on passive adversary model. Inn order to analyse the security needs of the MCPS passive adversary is widely used.

In cloud computing the problem related with privacy is based on multi-keyword searching over encrypted data. So it requires set of privacy requirements. It is done by an efficient method called ―coordinate matching,‖ . To quantitatively evaluate such similarity measure. The another method used is ―inner product similarity‖ . to achieve various stringent privacy requirements in two different threat models, here first propose a basic idea for the MRSE based on secure inner product computation.

S. Dziembowski proposed encryption mechanisms that pass through rigorous mathematical and theoretical cryptanalysis to provide security and privacy, the system may lost information due to the vulnerabilities in its software and hardware implementations. Attacks based on such leaked information are called side channel attacks. These attacks can be prevented by using leakage resistant cryptography [4].

In search of countermeasures, one can try to prevent side-channel attacks by modifying the implementation or securing hardware. This leads to a trial and error approach where an implementation is made secure against a certain type of attack only before a new more effective attack appears. Leakage Resilient Cryptography adopts a different viewpoint by trying to provide provably secure primitives in the presence of a wide range of side-channel information.

Designing measures are save in the presence of leakage is a difficult but not impossible task. The last few years, the cryptographic community has put a lot of effort in constructing leakage resilient primitives. As the foundations for a theoretical treatment of the subject have been set, we expect that within the next years more and more leakage resilient primitives will be constructed that will tolerate richer and richer families F of leakage functions.

Side channel attacks concentrate on obtaining the secret/ private key by using every layer of the system, rather than just the data that is being processed by the system. While many types of side channel attacks exist for nearly every encryption scheme.

Side-channel attacks[5] are arises due to software or hardware design problems. It is easy-to-implement against powerful attacks, and their targets includes primitives, protocols, modules, and devices to even systems. These attacks are causes Sevier problem to cryptographic sections. To avoid these problems some cryptographic analysis has to be considered. This involves the methods and techniques employed in these attacks, the destructive effects of such attacks, the countermeasures against such attacks and evaluation of their feasibility and applicability; Finally, the most important conclusion from this paper is that it is not only a necessity but also a must, in the coming version of FIPS 140-3 standard, to evaluate cryptographic modules for their prevention towards side channel attacks.

Timing attacks on elliptic curve cryptosystem target the scalar multiplication operation. It is prevented by using Montgomery's multiplication method which is proposed by P. L. Montgomery[6] performs the multiplication independent from the bits of the private key.

III.EXISTING SYSTEM

Establishing MCPSs will require overcoming technological hurdles in building the architectural components of the MCPS and assuring the privacy of the personal health information during the transmission from the sensory networks to the cloud and from the cloud to doctor’s mobile devices. Designing a MCPS involves survey on different encryption schemes and improvement of the usability of these schemes to provide secure storage, secure data sharing, and secure computation

IV.PROPOSED SYSTEM

With the above problem statement in order to overcome the privacy problem, the following objectives have been framed.

- The application is used to monitor the patient data and send that data on the cloud.
- To provide secure computation and storage requirements using AES in an MCPS.
- To provide privacy-preserving processing in a public cloud using advanced homomorphic encryption schemes.
- To facilitate decision support in cloud for healthcare professionals by applying critical system to the acquired data and predicting patient health condition.

V.METHODOLOGY

DATA PRIVACY

According to the Health Insurance Portability and Accountability Act (HIPAA), data privacy must be protected within every layer of an MCPS. Individual encryption schemes ensure that medical data is accessed by only the authorized parties, thereby providing data privacy on isolated data blocks. However, ensuring system level security requires designing a crypto-architecture for the MCPS as a whole.

KEY MANAGEMENT TECHNIQUES

Regardless of the type of encryption scheme, communicating parties must agree on key(s) to encrypt/decrypt messages. In the public-key cryptography, sender uses the public key of the receiver to encrypt messages and the receiver uses his/her private key to decrypt encrypted messages. Every user in the system has a dedicated public and private key pair generated by a Public-Key Infrastructure (PKI) [6]. PKI is a trusted third party such as a certificate authority that authenticates the key pairs by binding them to the identity of users.

For symmetric key cryptography, both sender and receiver must share the same secret key to encrypt/decrypt messages. Both parties perform a key-exchange protocol, such as Diffie- Hellman key exchange, to generate the secret key. Once both parties share the same key, they can use symmetric key cryptography to securely transfer the data.

The medical user or patient will send the data through smartphone, then that data is stored on the server. Homomorphic encryption schemes provide secure computation in a public cloud. The outcomes of the analytics or medical application results are given to the requesting authority to provide decision support about patient data. The System architecture is shown below in Fig 5.1.

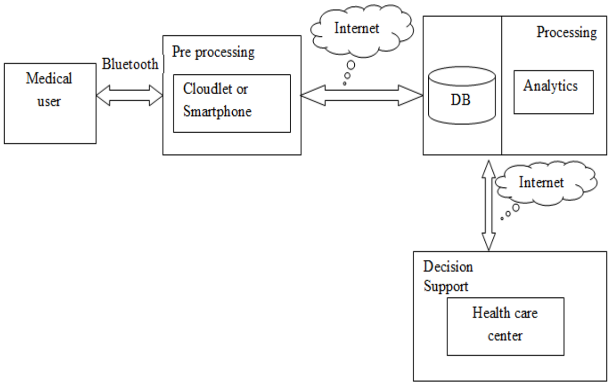


Fig 5.1: System Architecture

VI.CONCLUSION

The purpose this project is to save the life of critical stage patients and the authorized user can able to monitor the patient's details and their health condition continuously. Patient locality and health details are only visible for authorized users.Secure computation and storage requirements provided using AES encryption.The decision support is facilitated for healthcare professionals by applying critical system to the acquired data and predicting patient health condition.

If the patient is in critical health condition or the patient feels abnormal condition then the authorized users can gives the first aid, send the SMS to their relatives, and Authorized user will send the SMS to ambulance driver to pick up the patient.

REFERENCES

[1] A. Page, O. Kocabas, T. Soyata, M. K. Aktas, and J. Couderc, ―Cloud based privacy-preserving remote ECG monitoring and surveillance,‖ Ann. Noninvasive Electrocardiol., vol. 20 , no. 4, pp. 328 –337, 2014.
[2] 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.
[3] 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.
[4] S. Dziembowski and K. Pietrzak, ―Leakage-resilient cryptography,‖ in Proc. IEEE 49th Annu. IEEE Symp. Found. Comput. Sci., 2008, pp. 293–302.
[5] 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.
[6] P. L. Montgomery, ―Speeding the pollard and elliptic curve methods of factorization,‖ Math. Comput., vol. 48, no. 177, pp. 243–264, 1987.
[7] Lopez and R. Dahab, ―Fast multiplication on elliptic curves over GF(2m) without precomputation,‖ in Proc. Cryptographic Hardw. Embedded Syst., 1999, pp. 316 –327.
[8] T. S. Messerges, ―Securing the aes finalists against power analysis attacks,‖ in Proc . Fast Softw. Encryption, 2001, pp. 150 – 164 .
[9] J.S. Coron, ―Resistance against differential power analysis for elliptic curve cryptosystems,‖ in Proc. Cryptographic Hardw. Embedded Syst., 1999,
pp. 292 -302.
[10] W. Diffie and M. Hellman, ―New directions in cryptography,‖ IEEE Trans. Inf. Theor., vol. 22, no.6, pp. 644 –654, Nov. 2006.