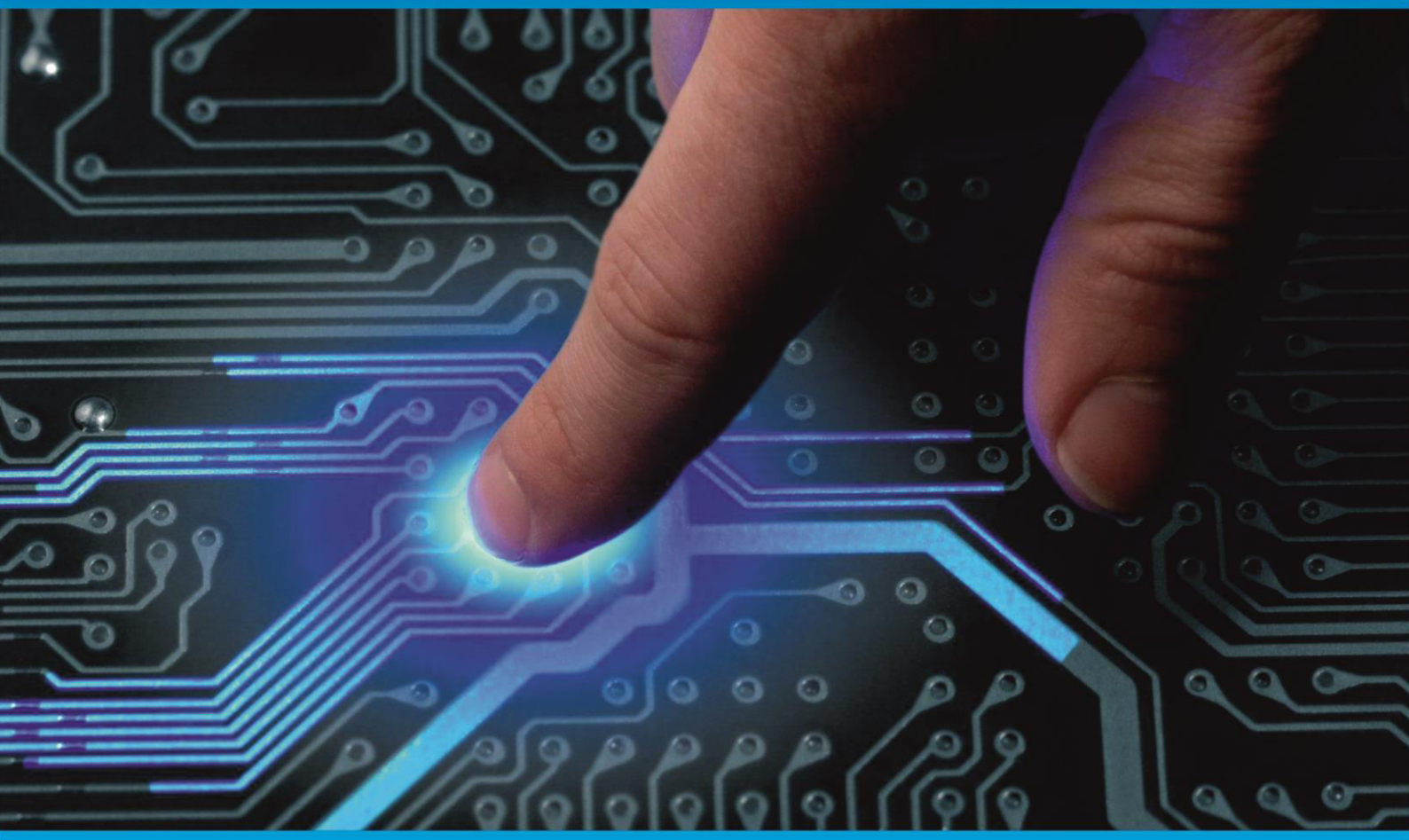
IJIRCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903094|

An Experimental Evaluation for Emerging Protection Mechanisms for Medical Cyber Physical Networks focused on IOT

Nivedita Singh[1], Pravin Kr Mishra[2]

M. Tech, Bharat Institute of Technology, Meerut, Dr. APJ Abdul Kalam Technical University, Lucknow, India[1]

Asst. Professor, Bharat Institute of Technology, Meerut, Dr. APJ Abdul Kalam Technical University, Lucknow, India[2]

ABSTRACT: In the ensuing decade, digital health tracking systems based on body-worn surveillance equipment have been growing. Those Medical Cyber Physical Systems (MCPS) move the collected data to a private or public cloud for preservation and retrieval. Medical practitioners may test the analysis of machine learning models in the cloud. In the implementation of MCPS the protection and confidentiality of medical knowledge is without question one of the key concerns. This proposal provides a general design of a four-layer MCPS: data collection, data aggregation, cloud management and actions. Owing to variations in the capacities of each layer's hardware and connectivity, multiple encryption schemes need to be used to ensure protection within the layer. We investigate conventional and new encryption schemes that rely on their capacity for cryptographic storage, data exchange and computer technologies. Our thorough experimental assessment on each system reveals that although modern features like secure sharing and secured computation enable evolving encryption schemes, multi-order calculations of magnitude and overhead storage are added. Finally, we describe possible study avenues to boost the usability of existing MCPS encryption schemes.

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

I. INTRODUCTION

MCPS development can avoid technological hurdles in developing architectural MCPS components such as sensors, cloud storage and easy Internet and smartphone access. In addition, ensuring the security of personal health information in conjunction with the transmission of sensory networks to the cloud and the construction of sophisticated cryptographic systems for MCPS from cloud to mobile devices by the doctor. Although this design needs protected storage using conventional encryption schemes, secure data sharing and safe computation alternatives are evolving encryption schemes.

The patient's networks can rapidly expand over the coming decade through cost-effective personal tracking systems that document numerous physiological signals like ECG and cardiac rates[1] or through advanced instruments able to quantify physiological indicators such as body temperature, skin resistance, gait, posture and EMG[2]. The advancement of these innovations and a perception of consumer value for personal health monitoring have also led to developments in rendering these devices trendy[3]. The unstoppable drive in designing such instruments has contributed to the creation of a full health monitoring device that is scientifically relevant to the patient. Medical information from patients may be passed on to private[4] or public cloud providers through a distributed sensor network. A number of cloud-based predictive inference algorithms can determine the relationship of patient data with current conditions[5]. This collaborations will be sponsored by medical practitioners to improve decision-making. This technology, called the Medical Cyber-Physical Systems (MCPS), represents the beginning of a new age of digital medicine and a technically-oriented human culture revolution. Establishing MCPSs will lead to technical difficulties in the building of architectural components for MCPS such as sensors, cloud storage architectures, fast Internet and wireless connectivity. The security of personal health details during transmission from sensory networks to clouds and from cloud to mobile medical devices often includes the sophisticated cryptographic architecture of MCPS. Although this design only involves protected storage utilizing traditional encryption mechanisms, modern encryption systems provide safe and reliable data exchange and measurement.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903094|

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 Annually rising corresponding study. As healthcare expenses escalate and the global population age, there is a need to track a patient's health condition when out of the hospital in his personal atmosphere. In order to satisfy this need, a number of device designs and consumer devices have been developed in recent years, with the goal of delivering diagnostic details in real time during analyzes, either to the patient or to a medical center or directly to a supervising healthcare provider, while being able to warn the client whether immediate health risks occur.

Wearable sensors have been more interested in recent years and many solutions for personal wellbeing, fitness and behaviour recognition are available today. 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. Using accessible knowledge and evidence obtained from device that often has access to a wide corpus of observation data for other people, the doctor may make a much stronger health prognosis and prescribe medication, early action, and life-style decisions that are especially successful in enhancing body fitness. Such a really helpful tool will enhance medical applications to ensure patient health status and trust. This may evoke fresh medical-science thoughts.

There are two models of aggressive adversary and passive adversary. The MCPS offers data protection on the aggressive adversary model[3], providing Privacy and correctness on the model of passive opponent. The security needs of the MCPS passive opponent are 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,‖ . Evaluating correlation test quantitatively. Another form is in-house product similarity. To satisfy numerous stringent privacy criteria in two separate threat models, first suggest a simple MRSE idea focused on stable internal product computation. S. Dziembowski suggested encryption systems that move through comprehensive mathematical and theoretical cryptanalysis to provide protection and secrecy, the device could loss information due to software and hardware implementation vulnerabilities. Attacks focused on such details are considered side-channel attacks. Using leakage-resistant cryptography[4] will avoid these assaults.

In pursuit of countermeasures, through changing deployment or protecting hardware, one may attempt to avoid side-channel assaults. This leads to a trial and error strategy where an architecture against a certain form of attack is rendered stable just until a new, more successful attack occurs. Leakage Resilient Cryptography takes a different perspective by attempting to provide provenly protected primitives with a broad range of side-channel details.
Designing steps as leakage happens is a challenging though not impossible job. The cryptographic group has placed a lot of work in building leakage resilient primitives in recent years. As the foundations for the theoretical treatment of the topic have been laid, we predict that more and more leakage-resilient primitives will be designed in the coming years to tolerate richer and richer families F leakage functions.

Side channel attacks concentrate on secret/private key extraction by utilizing some device layer other than the machine managed info. Though there are many kinds of side-channel attacks on almost every encryption device.

Side-channel attacks[5] trigger device or hardware design issues. It is simple to enforce against strong threats, like primitives, protocols, plugins, and devices to also programs. This attacks trigger serious cryptographic sections problem. Any cryptographic research must be known to prevent these issues. This includes methods and strategies used for these attacks, the disruptive results of such attacks, the anti-attack measures and the measurement of their viability and applicability; the most important conclusion of this document is that the next edition of FIPS 140-3 does not require cryptographic modules only.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903094|

Timing attacks on elliptic curve cryptosystem aim scalar multiplication. It is avoided using Montgomery's multiplication approach suggested by P. L. Montgomery[6] conducts multiplication independently of private key bits.

III. EXISTING SYSTEM

The creation of MCPSs will include solving technological problems in the architecture of the architectural MCPS components and ensuring the security of personal health information during transition from sensory networks to clouds and cloud to mobile medical devices. The architecture of the MCPS entails surveying and maximizing the performance of various encryption schemes for protected storage, secure data sharing and secure computation.

IV. PROPOSED SYSTEM

With the above problem statement to address the privacy question, the following goals were set.

- The program tracks patient data and transfers it to the cloud.
- Have stable processing and storage specifications utilizing MCPS AES.
- Offering public cloud privacy processing using sophisticated homomorphic encryption schemes.
- Promote cloud decision support for healthcare practitioners by adding vital frameworks to data collected and forecasting patient health status.

V. METHODOLOGY

DATA PRIVACY

Data security must be protected by each layer of MCPS under the Health Care Portability and Accountability Act (HIPAA). Personal encryption mechanisms ensure that the medical documents are read only by authorized individuals, ensuring privacy on isolated blocks of data. However, security at device level requires a crypto-architecture for the whole MCPS.

Key Management Techniques

Regardless of the encryption method sort, the coordinators will configure the key(s) to encrypt/decribe messages. The sender uses the public key of the receiver to encrypt public communications, while the recipient uses a private key to decode encrypted messages. A dedicated public and private key pair of PKIs per device user is created[6]. PKI is a trustworthy third party, like a certificate authority, that authenticates key pairs by connecting them to user identities.

Sender and recipient must share the same secret message key for symmetric key encryption/decryption. To generate the hidden key, all parties execute a key-exchange procedure like Diffie-Hellman key exchange. Upon exchanging the same key, both parties may use symmetric key cryptography to safely pass data.

The medical consumer or patient can submit the data to the server via smartphone. Homorphic encryption mechanisms guarantee safe cloud access. The study findings or the results of diagnostic applications are given to the requesting authority to endorse the judgment of patients. Figure 5.1 displays the architecture of the machine.

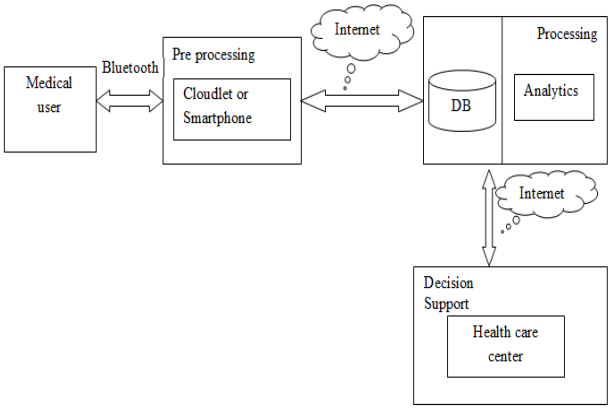


Fig 5.1: System Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903094|

VI. CONCLUSION

The goal of this project is to save the lives of vital patients and the approved consumer is able to actively track the patients' data and their wellbeing. Safe estimation and storage requirements given by AES encryption. The judgment support for health practitioners is supported by the implementation of critical framework to the acquired data and analysis of the patient health situation.

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, ―Cloudbased 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 andchallenges,‖ in Proc. IEEE Int. Conf. Serv. Comput., Jun. 2015, pp. 285–292.
[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ―Privacypreserving 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 theimpacts 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.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details