Energy efficient privacy preserving in Medical Cyber Physical Systems

Tanay Chillal[1], Ajinkya Mhatre[2], Dr. S.B Deshmukh[3]

[1]*Student, Pune Institute of Computer Technology, Pune*
[2]*Student, Pune Institute of Computer Technology, Pune*
[3]Professor, *Pune Institute of Computer Technology, Pune*

Abstract - *In the upcoming years, the Medical Cyber Physical Systems (MPCS) will have a huge impact in transforming the healthcare industry. The collected data can be sent by these MCPS to a public or private cloud for processing and archiving. Healthcare practitioners may receive decision support from machine learning algorithms processing this data on the cloud. In addition to it, algorithms running on cloud can provide predictive results based on the medical reports, patient data and background. These systems possess a problem of privacy breach as data to be computed is exposed to cloud vendors.*

Fully Homomorphic Encryption (FHE) solves this problem as it allows computations and operations to be performed on encrypted data, without decrypting the data, and without even needing the decryption key. In this paper, we discuss applications of homomorphic encryption in order to ensure privacy of sensitive medical data and survey conventional and emerging encryption schemes based on their ability to provide secure storage, data sharing, and secure computation. Privacy is preserved as cloud handles only the encrypted data and decryption is performed at the side of patient and authorized health professionals.

Key Words: **Medical cyber physical systems (MCPS), medical data privacy, homomorphic encryption, attribute-based encryption, disease risk prediction, Internet of Things (IoT).**

1.INTRODUCTION

In the healthcare domain, maintaining the confidentiality of sensitive patient records is paramount. Ensuring the privacy of such information is achievable through encryption, where the data owner encrypts the information before uploading it to a cloud service. This approach ensures that only the authorized data owner can access the data by decrypting it using their private decryption key. However, this encryption introduces challenges when it comes to outsourcing computations on externally stored information, particularly if the datacenter lacks access to the decryption key. Standard encryption schemes require the decryption key for performing computations on the data, making tasks like searching an encrypted database or conducting statistical analyses computationally intensive [1]. Nevertheless, these computational tasks are often essential for deriving business value from maintaining databases of customer or patient information. For instance, a hospital may seek performance evaluations based on patient health records without divulging specific details. Similarly, a patient may desire a centralized web service for storing and managing medical records while harboring concerns about the confidentiality of private health data. In such cases, obtaining health status information, such as disease predictions, becomes crucial [2]. Homomorphic encryption provides a solution by enabling computations on encrypted data without the need for decryption. This allows scenarios where a cloud prediction service can assess the likelihood of contracting a disease without exposing the actual medical record. The computation occurs without decrypting the data, and the result is delivered in encrypted form. The patient, upon receiving the encrypted prediction on a local device, decrypts it to access the prediction. This approach ensures that the cloud service only interacts with encrypted data, preserving the privacy of the underlying information [3].

Traditional encryption methods are highly efficient but lack the capability to perform computations on encrypted data. In contrast, homomorphic encryption (HE) schemes enable the execution of meaningful operations on encrypted data without revealing the actual information. By employing HE, both storage and computation tasks can be delegated to public cloud operators, addressing concerns related to data privacy in medical cloud computing. A Fully Homomorphic Encryption (FHE) scheme is achieved when it can evaluate arbitrary functions. To perform such evaluations on ciphertexts, FHE schemes must conduct both homomorphic addition and homomorphic multiplication, equivalent to the addition and multiplication of plaintext messages, respectively [4][5].

The initial viable FHE scheme was introduced by Gentry in 2009. Preceding schemes were partially homomorphic, capable of either homomorphic addition or homomorphic multiplication exclusively. The Paillier scheme is solely additively homomorphic, allowing only addition operations on ciphertexts. On the other hand, FHE facilitates both homomorphic additions and multiplications, enabling arbitrarily complex computations. Presently, FHE schemes are not practical due to their demanding computational and storage requirements. Ongoing research efforts are dedicated to enhancing the performance of FHE. This section delves into the details of the Paillier scheme and a recent FHE implementation known as the Brakerski-Gentry-Vaikuntanathan (BGV) scheme [3][23].

1.1 Paillier Encryption Scheme

Paillier Encryption scheme is a public-key cryptosytem that is additively-homomorphic. Operations on ciphertexts encrypted with Paillier scheme result in additions of messages without observing them [3]. Due to its additive homomorphism, Paillier scheme is widely used in many practical applications. Security of the Paillier scheme is based on difficulty of finding the nth residue of composite numbers [3][6]:

Given z and n 2 where n = p · q is a composite number, it is hard to find y that observes the following relationship

$$z = y^n \bmod n^2$$

1.2 BGV Scheme

Several FHE implementations have been proposed to date to improve performance of Gentry's initial FHE scheme. Currently, the BGV scheme is one of the most promising candidates for a practical FHE scheme, incorporating many optimizations. The expensive bootstrapping operation is avoided by a variant of FHE called leveled FHE that employs a better noise management technique called modulus-switching. Cipher�texts encrypt multiple messages to reduce storage overhead and execute homomorphic operations in parallel similar to SIMD-fashion [20][21][22].

2. Literature Survey

The field of Medical Cyber Physical Systems (MCPS) has witnessed significant growth, with the development of systems that monitor patients through cost-effective, body�worn personal devices capturing multiple physiological signals like ECG and heart rate. Additionally, more advanced devices are available, measuring diverse physiological markers such as body temperature, skin resistance, gait, posture, and EMG [8]. The emergence of these devices, coupled with increased user awareness of their importance in personal health monitoring, has propelled the relentless progress in constructing comprehensive patient health monitoring systems suitable for clinical use [9][10]. In these systems, medical data collected from patients through a distributed sensor network can be transmitted to either private or public cloud services. Within the cloud, a set of statistical inference algorithms operates to establish correlations between patient data and known disease states [12]. These correlations can then be relayed to healthcare professionals, serving as valuable information for decision support. This integration of devices and cloud-based analysis characterizes the Medical Cyber-Physical Systems (MCPS) [13][15].

2.1 Architecture of MCPS

The architecture of Medical Cyber-Physical Systems (MCPS) typically comprises four distinct layers, each playing a crucial role:

Data Acquisition Layer

This layer, often a Body Area Network (BAN), involves wireless wearable sensors for specific medical applications like monitoring blood pressure and body temperature.[8] BAN facilitates the collection of patient medical information, forwarding it to a nearby computationally-capable device, such as a cloudlet. Battery-operated active sensors in the BAN utilize Bluetooth or ZigBee protocols, while battery-less passive sensors employ RFID [11][12].

Data Concentration/Aggregation Layer

Due to the limited computational power of BAN sensors, an intermediate device, either a cloudlet or a concentrator, becomes necessary. Sensors transmit gathered information to a gateway server (concentrator) through a Bluetooth connection [12]. The concentrator is a vital component of an IoT-based architecture, enabling individually weak devices to exhibit strong overall functionality by concentrating data and sending aggregated information to the cloud. A cloudlet serves a similar purpose but aggregates data from more powerful devices like smartphones. It is typically constructed from a dedicated computer with a dedicated Internet connection [14][15].

Cloud Processing and Storage Layer

The cloud's primary functions include secure storage, crucial for accurate diagnosis requiring long-term patient health monitoring information [14][15]. Government health regulations mandate the storage of medical records for an extended period. Many cloud operators sign Business Associate Agreements (BAA) to store medical data securely. Medical institutions utilize private clouds (datacenters) for running applications, employing the cloud's second significant purpose: processing. Privacy preserving processing in a public cloud is feasible through advanced homomorphic encryption schemes. The cloud's third function involves data analytics, facilitating decision support for healthcare professionals. Statistical inference algorithms are applied to acquired data to predict patient health conditions, particularly emphasized in remote health monitoring systems [16][17].

Action Layer

The action layer can provide either "active" or "passive" action. In active action, an actuator, such as a robotic arm, is activated based on the results of algorithms running in the cloud. Examples include robot-assisted surgery [17]. In passive action, no physical action occurs. The outcomes of analytics or medical application results are presented to the requesting authority to provide decision support. An example is the visualization of a patient's long-term (24-hr) Holter ECG monitoring, allowing a doctor to review 20-30 patients' results within 10-20 seconds [22].

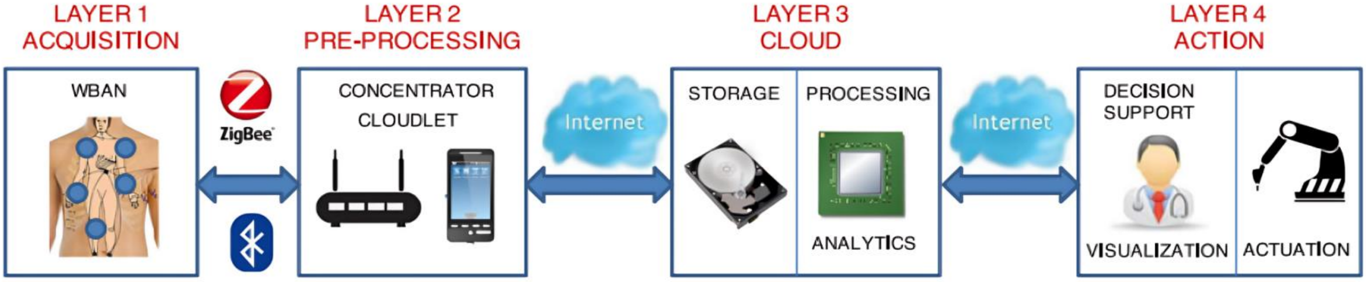

Fig. 1 Four layers of a typical Medical Cyber Physical System.

2.2 DATA PRIVACY IN AN MCPS

Adhering to the Health Insurance Portability and Accountability Act (HIPAA), safeguarding data privacy within every layer of an MCPS is imperative. Individual encryption schemes guarantee that access to medical data is limited to authorized parties, ensuring data privacy specifically on isolated data blocks. However, establishing system-level security necessitates the formulation of a comprehensive crypto-architecture for the MCPS as a unified entity.

Key Management Techniques

Irrespective of the chosen encryption scheme, parties involved in communication must mutually agree on keys for encrypting/decrypting messages. In public-key cryptography, the sender utilizes the recipient's public key for encryption, while the recipient uses their private key for decryption. Each user possesses a dedicated public and private key pair generated by a Public-Key Infrastructure (PKI), a trusted third party like a certificate authority that authenticates the key pairs by associating them with user identities. For symmetric-key cryptography, both sender and recipient share the same secret key, generated through a key-exchange protocol such as Diffie-Hellman [3].

Data Acquisition Privacy

The acquisition layer in Fig. 1 comprises BAN sensor devices with restricted computational capability and battery life [19]. Consequently, encryption schemes safeguarding communication within BAN sensors and BAN-to-cloudlet communications should avoid being computationally intensive. One viable option is employing the Zigbee protocol based on the AES encryption scheme, which can be easily implemented using cost-effective microcontroller-based devices. Secure communication between devices can also be achieved by utilizing biomedical signals. For instance, in [19], authors propose a low-power bio-identification mechanism using the interpulse interval (IPI) to secure communication between BAN sensors.

Data Sharing Privacy

In various real-world healthcare scenarios, multiple entities may need access to data, including the patient being monitored, their doctor, and, in emergencies, other healthcare personnel. Conventional encryption schemes face challenges in handling the sharing of the secret key among multiple parties. Encrypting data using each party's public key is not a viable solution as it results in data duplicates, necessitating separate management. Attribute-based encryption (ABE) emerges as a solution, allowing secure data sharing among multiple parties. ABE, a public-key crypto-system, provides fine-grained access control similar to Role-Based Access Control [18][20]. In [21], authors propose methods to secure data storage in BANs and distribute data access control, using the ABE scheme to control who accesses patient data. ABE encryption is applied to data on a nearby local server, and communication between the BAN and the local server is secured using symmetric key encryption.

Data Computation Privacy

Conventional encryption schemes fall short in enabling computations on encrypted data without prior decryption, requiring trusted storage like healthcare organizations' data centers or private clouds. This limitation prevents the execution of analytics, monitoring algorithms (e.g., ECG monitoring), or other algorithms in a public cloud, hindering potential cost reduction in healthcare [9]. Fully Homomorphic Encryption (FHE) emerges as a solution, allowing computation on encrypted data. By utilizing FHE, data can be stored in untrusted storage environments like public clouds, and computations on encrypted data can be executed without compromising data privacy [21]. In [23], a privacy-preserving medical cloud computing system is proposed based on FHE, demonstrating that even complex operations, such as computing average, minimum, and maximum heart rates, can be implemented at a reasonable cost. In Paper [23], an MCPS is described as a remote health monitoring system taking inputs from the patient's body (Layer 1) and transmitting to the cloud (Layer 3). Patient medical data should be encrypted using homomorphic encryption schemes for data privacy. Despite the resource-intensive nature of HE schemes, an intermediate preprocessing layer is proposed to support HE computationally. The recordings will be stored and processed in the cloud to provide statistics and detection results to doctors, including the assessment of long-term problems based on parameters like average heart rate and ECG recordings.

3. Proposed Methodology

In the Data Concentration/Aggregation Layer, data collected from wearable sensors, using protocols like Zigbee and Bluetooth, is processed since sensors lack the computational capability to directly transmit data to the cloud. Within this layer, the cloudlet or smartphone plays a pivotal role in IoT-based architecture.

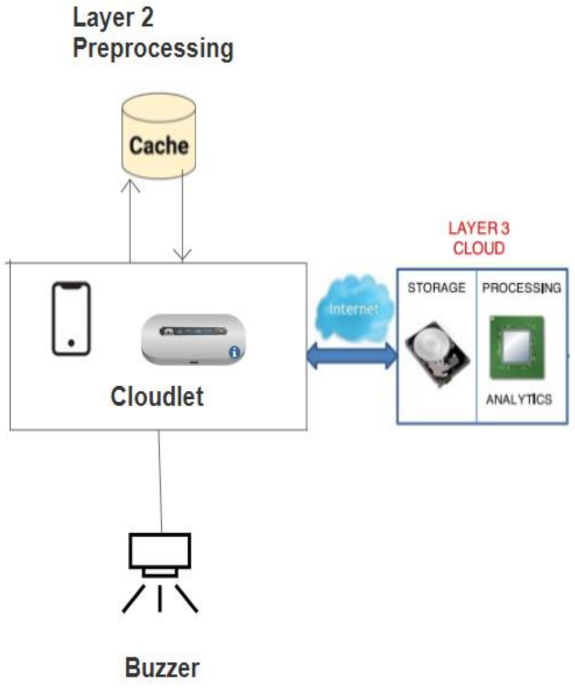

Fig .2 Layer 2 and Layer 3 of MCPS Architecture with Cache and buzzer

In the Data Concentration/Aggregation Layer, data collected from wearable sensors, using protocols like Zigbee and Bluetooth, is processed since sensors lack the computational capability to directly transmit data to the cloud. Within this layer, the cloudlet or smartphone plays a pivotal role in IoT-based architecture. However, it currently transmits data for all health parameters at fixed intervals to the cloud, which may not always be necessary. Minor fluctuations in parameters, such as a shift in heart rate from 90 to 88 or a change in body temperature from 36°C to 36.5°C, are not crucial for predictive analysis. This inefficiency results in increased energy consumption, as redundant and insignificant data is sent to the cloud, leading to a heavier load and faster battery drainage in the cloudlet, consuming more electricity.

To address this issue, we propose implementing a cache for each health parameter in the cloudlet. This approach would ensure that only significant spikes and gradual changes in readings are captured and transmitted to the Third Layer (Cloud). Instances where the heart rate abruptly increases from 90 to 100 or drops to 80, or when body temperature shifts from 36°C to 39°C, would be selectively sent to the Third Layer for prediction and processing. This modification aims to reduce computational overhead both at the cloud and the cloudlet, as plaintext data need not be encrypted and transmitted unnecessarily. Additionally, we suggest enhancing the system by connecting the cloudlet to a buzzer. This feature would enable the system to generate an alert in cases where sensor readings fall below a minimum threshold or surpass a maximum threshold. The buzzer's noise could serve as a prompt for medical staff present, allowing them to provide personalized assistance to the patient.

These proposed improvements in the Medical Cyber-Physical System (MCPS) aim to enhance energy efficiency, reduce unnecessary data transmission, and provide more focused attention to the patient.

4. Conclusion and Future Scope

4.1 Conclusion

In this paper, we have surveyed implementation of Medical Cyber Physical Systems (MCPS) employing cloud ensuring privacy preserving using Homomorphic encryption. Unlike conventional encryptions such as AES and ECIES, it allows the cloud to perform computations on encrypted data to provide private predictive analysis.

4.2 Future Scope

The upcoming years will see a rise in systems that monitor a patient through body-worn inexpensive personal monitoring devices that record multiple physiological signals, such as ECG and heart rate or more sophisticated devices that measure physiological markers such as body temperature, skin resistance, gait, posture, and EMG. This will enable the construction of complete patient health monitoring systems and provide private predictive analysis.

ACKNOWLEDGEMENT

We express our gratitude to the Department of Information Technology at PICT, Pune for their unwavering support and invaluable guidance during the course of this work. The department's assistance has been instrumental in its fruition. Additionally, our heartfelt appreciation extends to our esteemed guide, Dr. S.B. Deshmukh, whose expert mentorship played a pivotal role in shaping this endeavor. His profound insights and continuous support have been invaluable, ensuring the success of our research paper. We are sincerely thankful for her unwavering dedication and guidance throughout our research journey.

REFERENCES

[1] Joppe W. Bos, Kristin Lauter, Michael Naehrig, " Private predictive analysis on encrypted medical data" in Journal of Biomedical Informatics.

[2] Benaloh J, Chase M, Horvitz E, Lauter K. "Patient controlled encryption: ensuring privacy of electronic medical records" in Proceedings of the first ACM cloud computing security workshop – CCSW. ACM; 2009. p. 103–14.

[3] Xun Yi, Russell Paulet, Elisa Bertino "Homomorphic Encryption and Applications" Springer

[4] 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

[5] Ovunc Kocabas, Tolga Soyata, and Mehmet K. Aktas "Emerging Security Mechanisms for Medical Cyber Physical Systems" in IEEE/ACM TRANSACTIONS ON COMPUTATIONAL BIOLOGY AND BIOINFORMATICS, VOL. 13

[6] O. Kocabas, R. Gyampoh-Vidogah, and T. Soyata, "Operational cost of running real-time mobile cloud applications," in Enabling Real-Time Mobile Cloud Com�puting through Emerging Technologies., T. Soyata, Ed. Hershey, PA, USA: IGI Global, 2015, ch. 10, pp. 294–321

[7] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Process. Mag., vol. 30, no. 1, pp. 82–105, Jan. 2013

[8] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," IEEE Trans. Sys., Man, Cybern., Part C: Appl. Rev., vol. 40, no. 1, pp. 1–12, Jan. 2010.

[9] 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

[10] 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.

[11] A. Benharref and M. A. Serhani, "Novel cloud and SOA-based framework for E�Health monitoring using wireless biosensors," IEEE J. Biomed. Health Inf., vol. 18, no. 1, pp. 46–55, Jan. 2014.

[12] S. Babu, M. Chandini, P. Lavanya, K. Ganapathy, and V. Vaidehi, "Cloud-enabled remote health monitoring system," in Proc. Int. Conf. Recent Trends Inform. Tech., Jul. 2013, pp. 702–707.

[13] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A cloud computing solution for patient's data collection in health care institutions," in Proc. Int. Conf. eHealth, Telemed., Social Med., Feb. 2010, pp. 95–99.

[14] G. Nalinipriya and K. R. Aswin, "Extensive medical data storage with prominent symmetric algorithms on cloud - a protected framework," in Proc. IEEE Int. Conf. Smart Struct. Syst., Mar. 2013, pp. 171–177.

[15] A. F. Hani, I. V. Paputungan, M. F. Hassan, V. S. Asirvadam, and M. Daharus, "Development of private cloud storage for medical image research data," in Proc. Int. Conf. Comput. Inf. Sci., Jun. 2014, pp. 1–6.

[16] O. Kocabas and T. Soyata, "Medical data analytics in the cloud using homomorphic encryption," in Handbook of Research on Cloud Infrastructures for Big Data Analytics, P. R. Chelliah and G. Deka, Eds. Hershey, PA, USA: IGI Global, Mar. 2014, ch. 19, pp. 471–488

[17] B. Rao, "The role of medical data analytics in reducing health fraud and improving clinical and financial outcomes," in Proc. IEEE 26th Int. Symp. Computation-Based Med. Syst., Jun. 2013, pp. 3–3.

[18] C. Poon, Y. Zhang, and S. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," IEEE Commun. Mag., vol. 44, no. 4, pp. 73–81, Apr. 2006.

[19] K. K. Venkatasubramanian, A. Banerjee, and S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," IEEE Trans. Inf. Technol. Biomed., vol. 14, no. 1, pp. 60– 68, Jan. 2010.

[20] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[21] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[22] A. Page, T. Soyata, J. Couderc, M. Aktas, B. Kantarci, and S. Andreescu, "Visualization of health monitoring data acquired

from distributed sensors for multiple patients,” in Proccedings. IEEE Global Telecommunication. Conference., Dec. 2015.

[23] Ovunc Kocabas, Tolga Soyata, and Mehmet K. Aktas “Emerging Security Mechanisms for Medical Cyber Physical Systems” IEEE/ACM TRANSACTIONS ON COMPUTATIONAL BIOLOGY AND BIOINFORMATICS