



IJIRCCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 2, February 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.488

 9940 572 462

 6381 907 438

 ijircce@gmail.com

 www.ijircce.com

Security Mechanism For Medical Cyber Physical Systems Using Encryption

Arun Kumar¹, Prof. Sunil Kumar Mishra²

M. Tech, Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University,
Lucknow India¹

Asst. Professor, Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University,
Lucknow, India²

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 paper, 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 (MCPS), Health-monitoring, Machine learning

I. INTRODUCTION

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. 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

II. LITERATURE SURVEY

In 2015, N. Powers et al [1], presented a mobile-cloudlet-cloud architecture to perform real-time face recognition by executing this application in three distinct steps: Face Detection (FD), Projection (PJ) and Searching (S). We observed that, due to their separability, these three steps can be executed in different hardware components: Mobile device (M), Cloudlet (CL), and Cloud (C).

In 2014, A.F. Hani, I. V. Paputungan, M. [2], presented a private cloud storage design and prototype development within an organization to solve such issues. Leveraging on the ability of cloud computing is shown meet to the system requirements. The prototype is implemented on OwnCloud cloud storage framework. The complete functionality of OwnCloud made it an ideal platform to develop and deploy this kind of cloud-based system. OwnCloud can keep images in different file formats and share such images to other.

In 2014, S. X. et al [3] described experimental and theoretical approaches for using ideas in soft microfluidics, structured adhesive surfaces, and controlled mechanical buckling to achieve ultralow modulus, highly stretchable systems that incorporate assemblies of high-modulus, rigid, state-of-the-art functional elements. The outcome is a thin, conformable device technology that can softly laminate onto the surface of the skin to enable advanced, multifunctional operation for physiological monitoring in a wireless mode.

In 2014, A. Page et al [4], proposed a system that couples health monitoring techniques with analytic methods to permit the extraction of relevant information from patient data without compromising privacy. The proposal is based on the concept of fully homomorphic encryption (FHE). Since the technique is known to be resource-heavy, the papers develop a proof-of-concept to assess its practicality. Results are presented from proposed prototype system, which mimics live QT monitoring and detection of drug induced QT prolongation.

In 2014, A. Benharref and M. A. Serhani [5], proposed a framework to collect patients' data in real time, perform appropriate non-intrusive monitoring, and propose medical and/or life style engagements whenever needed and appropriate. The framework, which relies on Service Oriented Architecture (SOA) and the Cloud, allows a seamless integration of different technologies, applications, and services. It also integrates mobile technologies to smoothly collect and communicate vital data from a patient's wearable Biosensors while considering the mobile devices' limited capabilities and power drainage in addition to intermittent network disconnections. Then data is stored in the Cloud and made available via SOA to allow easy access by physicians, paramedics or any other authorized entity.

In 2014, N. Cao et al [6], defined and solved the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). The proposed papers establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, the paper choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. In further use "inner product similarity" to quantitatively evaluate such similarity measure. paper first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models.

In 2013, S. Babu et al [7], Proposed Open Geo-Spatial Consortium (OGC) standard based remote health monitoring system that allows integration of sensor and web using standard web-based interface. The aim is to provide the data in an open & interoperable manner, and reduce data redundancy. Fixed specification is used for exchange of sensor data globally for all sensor networks. OGC SWE is applicable to different sensor systems including medical sensor networks. A standard format is used to document sensor descriptions and encapsulate data. Sensor data is ported on to cloud which provides scalability, centralized user access, persistent data storage and no infrastructure maintenance cost for heavy volumes of sensitive health data. Decision tree pruning algorithm with high confidence factor is proposed for automatic decision making.

In 2013, C. O. Rolim et al [8], proposed a solution to automate this process by using “sensors” attached to existing medical equipment that are inter-connected to exchange service. The proposal is based on the concepts of utility computing and wireless sensor networks. The information becomes available in the “cloud” from where it can be processed by expert systems and/or distributed to medical staff. The proof-of-concept design applies commodity computing integrated to legacy medical devices, ensuring cost effectiveness and simple integration.

In 2012, D. Kim et al [9], Advances in materials, mechanics, and manufacturing now allow construction of high-quality electronics and optoelectronics in forms that can readily integrate with the soft, curvilinear, and time-dynamic surfaces of the human body. The resulting capabilities create new opportunities for studying disease states, improving surgical procedures, monitoring health/wellness, establishing human-machine interfaces, and performing other functions. Above review summarizes these technologies and illustrates their use in forms integrated with the brain, the heart, and the skin.

In 2012, T. Soyata et al [10], designed and implemented the MOCHA Architecture: mobile devices interact with the cloudlet and the cloud via multiple connections and use dynamic partitioning to achieve their QoS goals (e.g., latency, cost).

III. RESEARCH METHODOLOGY

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.

Modules formalized

- **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 preparation of an assembly of methods, procedures, or techniques united by regulated interaction to form an organized whole is termed as Systems design. It is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements.

Systems design could be seen as the application of systems theory to product development. The design process translates the requirements into a representation of the software that can be assessed for quality before coding begins. Once the requirements have been collected and analysed, it is necessary to identify in detail how the system will be constructed to perform the necessary tasks.

The system design transforms a logical representation of what a given system is required to be in to physical specification. Design starts with the system's requirement specifications and converts it into a physical reality during the development. Various design features are followed to develop the system. The design specification describes the features of the system, the components or elements of the system and their appearance to end users.

4.1 DATA FLOW DIAGRAMS

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design).

A DFD shows what kinds of information will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.

4.1.1 Data Flow Diagram for Admin Module

The Level 1 DFD shows how the system is divided into sub-systems (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

Here Admin login with the id and password. After login Admin can add the location, add trusted user, view the patient details and also can change the password. The DFD for admin module is given in Fig 4.1.1.

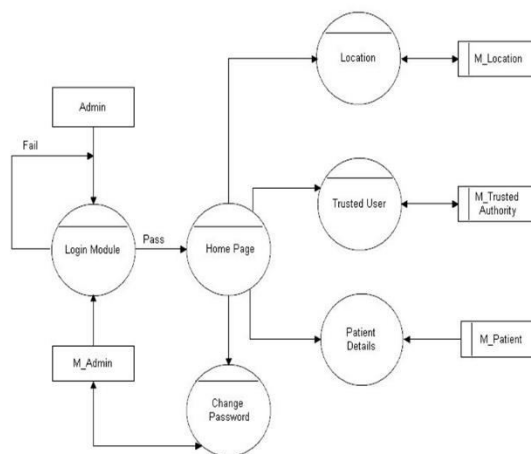


Fig 4.1.1: Data flow diagram for Admin Module.

4.1.2 Data flow Diagram for Trusted User Module:

Trusted user login with the user id and password. After login Trusted User can add the Patient Details, ambulance details and view the patient recording if the data is critical sends the message to the ambulance and also can change the password. The DFD for Trusted User module is given in Fig 4.1.2.

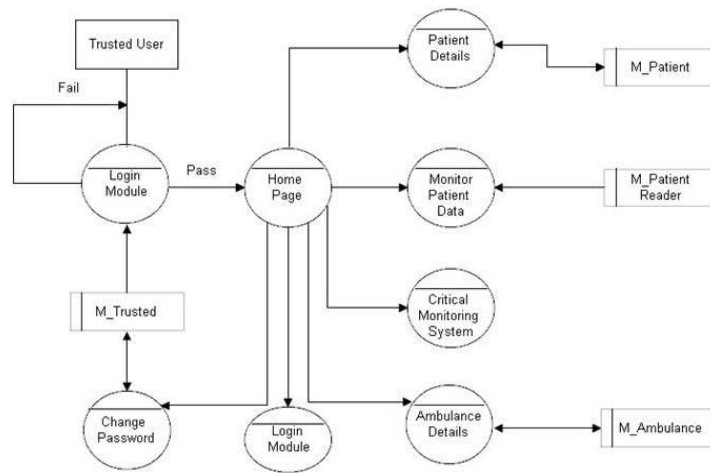


Fig 4.1.2: Data flow diagram for Trusted User module

4.1.3 DFD for Android: Patient Module

Patient login with the user id and password. After login Patient can start entering the data and also can change the password. The data flow diagram for Patient is given in Fig 4.1.3.

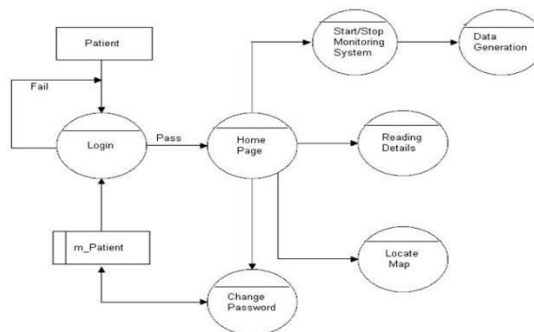


Fig 4.1.3: Data flow diagram for Patient.

V. AES ENCRYPTION ALGORITHM

AES is one of the most widely used symmetric key encryption algorithms and is accepted as an industry and a government applications standard. AES is optimized for speed, low memory footprint and energy efficiency. Its low resource intensity allows AES to run on a wide range of hardware platforms ranging from 8-bit microcontrollers to high-end desktops and servers.

ALGORITHM:

Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])

Begin

byte state[16];

```
state = in;  
  
AddRoundKey(state, round_key[0]);  
  
for i = 1 to Nr-1 stepsize 1 do  
  
    SubBytes(state);  
  
    ShiftRows(state);  
  
    MixColumns(state);  
  
    AddRoundKey(state, round_key[i]);  
  
end for  
  
subBytes(state);  
  
ShiftRows(state);  
  
AddRoundKey(state, round_key[Nr]);  
  
End
```

VI. EXPERIMENTAL RESULTS

6.1 Patient Login Page

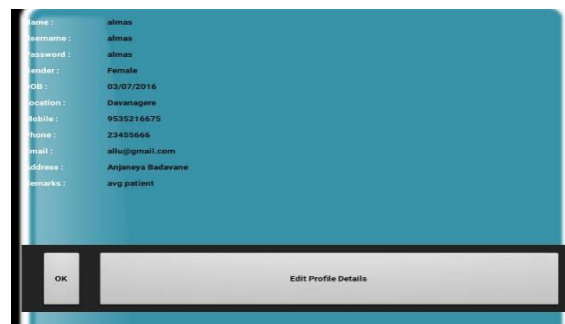


The screenshot shows a web interface for patient login. At the top, there is a blue header with a globe icon and the text 'Mobile healthcare'. Below the header is a small cartoon character. The main content area contains two input fields: 'Username' with the text 'almas' and 'Password' with five dots. A green 'Login' button is positioned below the password field.

Fig : Patient Login Page

Fig is the Patient Login page. Here patient can login with username and password.

Patient Profile Details



The screenshot displays a patient profile details page. The background is a light blue gradient. The profile information is listed in a table-like format:

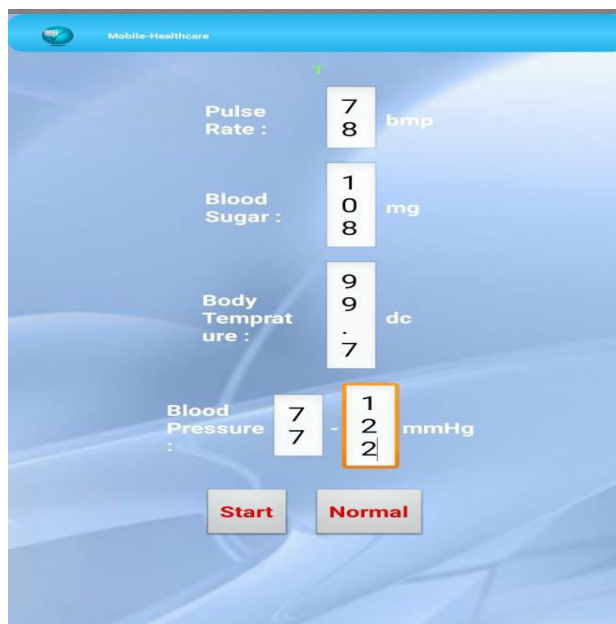
name :	almas
username :	almas
password :	almas
gender :	Female
DOB :	03/07/2016
location :	Davanagere
Mobile :	9535216675
Phone :	23495666
email :	almas@gmail.com
address :	Anjaneya Badavane
remarks :	avg patient

At the bottom of the page, there are two buttons: 'OK' and 'Edit Profile Details'.

Fig: Patient Profile Details

In Fig patient can view the profile details and also can edit the details if required.

Data Monitoring Page



Pulse Rate :	78	bmp
Blood Sugar :	108	mg
Body Temperature :	99.7	dc
Blood Pressure :	77/122	mmHg

Buttons: Start, Normal

Fig 7.3.3: Data Monitoring Page

Fig is the data entering page. Here Patient can enter the details such as, pulse rate, blood sugar, body temperature and blood pressure.

VII. 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] Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain –Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3,
- [2] Pavel Tarasov and Hitesh Tewari(2017);The Future of E-Voting; IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165 I
- [3] Zibin Zheng¹, Shaoan Xie¹, Hongning Dai², Xiangping Chen⁴, and Huaimin Wang³(2017);An Overview of Blockchain Technology : Architecture,Consensus, and Future Trends; IEEE 6th International Congress on Big Data.
- [4] Jesse Yli-Huumo¹, Deokyoon Ko², Sujin Choi^{4*}, Sooyong Park², Kari Smolander³(2016); Where Is Current Research on Blockchain Technology?—A Systematic Review;PLOS-ONE.
- [5] Mahdi H. Mirazl¹, Maaruf Ali²(2018); Applications of Blockchain Technology beyond Cryptocurrency;Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018
- [6] Michael Crosby, Google,Nachiappan, Yahoo,Pradhan Pattanayak, Yahoo,Sanjeev Verma, Samsung Research America,Vignesh Kalyanaraman, Fairchild Semiconductor(2015);Blockchain Technology Beyond Bitcoin.
- [7] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis (2018); E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy; arXiv:1805.10258v2 [cs.CR]
- [8] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim(2016); Electronic Voting Service Using Block-Chain; Journal of Digital Forensics, Security and Law.



- [9] Aayushi Gupta^{1*}, Jyotirmay Patel², Mansi Gupta¹, Harshit Gupta¹(2017); Issues and Effectiveness of Blockchain Technology on Digital Voting; International Journal of Engineering and Manufacturing Science. ISSN 2249-3115 Vol. 7, No. 1 (2017)
- [10] Gautam Srivastava¹, Ashutosh Dhar Dwivedi² and Rajani Singh²(2018); Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology.
- [11] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson(2018);Blockchain-Based E-Voting System.
- [12] Nir Kshetri and Jeffrey voas(2018);Blockchain Enabled E-Voting;www.computer.org/software.
- [13] Umut Can Çabuk¹, Eylül Adıgüzel², Enis Karaarslan²(2018); A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems; International Journal of Advanced Research in Computer and Communication Engineering.
- [14] Madise, Ü. & Martens, T. (2006). E-voting in Estonia 2005. The first practice of countrywide binding Internet voting in the world. Electronic Voting, 86.
- [15] S. Raval, “Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology.” O’Reilly Media, Inc. Sebastopol, California (2016).
- [16] Jason Paul Cruz^{1,a} Yuichi Kaji^{2,b}(2017);E-voting System Based on the Bitcoin Protocol and Blind Signatures ; IPSJ Transactions on Mathematical Modeling and Its Applications Vol.10 No.1 14–22.
- [17]<https://www.google.com/A+Simple+Representation+of+the+Blockchain+Structure+of+each+Candidate+in+e+voting>



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



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