Research Article

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology

2020
Vol.8 No.1:46

DOI: 10.36648/2349-3917.8.1.46

Comparative Analysis of Encryption Techniques for Sharing Data in IoMT Devices

M Asad Bilal[1*] and Sidra Hameed[2]

[1]Imperial University Lahore, Lahore, Pakistan

[2]Degree College Noshehra Road Gujrawala, Lahore, Pakistan

[*]**Corresponding author:** M Asad Bilal, Lecturer in Imperial University Lahore, Lahore, Pakistan, E-mail: asadbilal4@gmail.com

Received date: February 10, 2020; **Accepted date:** February 25, 2020; **Published date:** March 02, 2020

Citation: Bilal MA, Hameed S (2020) Comparative Analysis of Encryption Techniques for Sharing Data in IoMT Devices. Am J Compt Sci Inform Technol Vol.8 No.1: 46

Abstract

IoT healthcare devices are being used to share the real time personal data of patients to their doctors. Conventionally, centralized systems are used to store personal data and for encryption decryption, property server performed the duty. But those systems give rise to security and response time issues e.g. data breaching while moving the data between devices and server as there are IoT devices which send their data (blood pressure, heart beat rate etc.) as plain text to server and server have to perform encryption/decryption according to the need. Apart this, server have to response back the requests of different healthcare provider's devices which may increase the response time. Therefore, security and response time are the main issues to be handled. There is a need of system that makes the secure transmission of sensitive healthcare data. We recommend some suggestions to improve those areas.

Keywords: Internet of things (IoT); Security; Encryption; Privacy; Internet of medical things (IoMT)

Introduction

Many healthcare providers are utilizing Internet of medical things applications to improve treatments, manage diseases, reduce errors, improve patient experience, manage drugs, and reduce the cost [1]. According to market research (Big Data in Internet of Things (IoT): Key Trends, Opportunities and Market Forecasts 2015 – 2020 n.d), the healthcare IoT market segment is poised to reach $117 billion by 2020. P and S Market Research submitted a report according to which there will be a compound annual growth rate (CAGR) of 37.6% in the healthcare Internet of Things industry between the years 2015 and 2020 [2].They claim that this rise could be attributed to the upper hand of remote monitoring healthcare systems that can detect chronic life-threatening diseases. By this we can assume that IoT has taken the reins and people can enjoy personalized attention for their health requirements; they can tune their devices to remind them of their appointments, calorie count, exercise check, blood pressure variations and so much more. New security issues related to confidentiality, integrity, and availability (CIA) arise. Since most IoT components transmit and receive data through wireless nature, this puts IoMT in danger of wireless sensor network (WSN) security violations [3]. IoT health applications and data store and transmit in the cloud effected by severe cyber-attacks Alasmari et al. [4]. All these issues relate to security and privacy of patient's data. Attacks on different connected devices affect the integrity and privacy of patient's data which may also cause the undesirable results [1].

Literature Review

Internet of things first coined in 1999 and gained lot of publicity from any kind of business to government. It refers to the connectivity among different devices through a network-using internet [5]. Internet of medical things is innovative concept in IoT having different applications like newer product development, real time data generation, treatment adherence monitoring, smarter decision taking applicability in the hands of healthcare provider, improved healthcare infrastructure and Customized product development and care. Keeping all these advantages in mind IOMT also have to face challenge of data integration and data management. Data security and privacy is a big concern here which is affecting the lives of many patients.

Quality patient care requires an important role of advance technologies of interconnected medical devices and sensors [6]. This healthcare system is a combination of communication devices, interconnected applications, devices, sensors and people that would function together as one smart system to monitor, track, and store patients' healthcare information for on-going care. Writer proposed a cloud based framework to securely transfer medical data from mobile devices and other sensors to provide access to medical professionals. Identity theft is protected using watermarking and signal enhancement. Concerned study is using watermarking before sending the data to cloud which is an old technique to secure the data. Further studies also proved that watermarking is not secure if the opponent refines his knowledge on the presumably secret key.

Hospitals and Medical care providers are obligated to exchange patients' private information securely to comply with HIPAA [4]. Security and privacy concern will grow as e-health

clouds are going to be widely implemented to host not only applications but also software development tools and APIs. The use of hybrid cloud (using private and public cloud) will also exacerbate the security situation causing billions of confidential data to be stored and transferred in cloud servers. Patients' sensitive personal and medical information could be a tampered, used or compromised in the absence of having real time monitoring. Therefore, Cloud companies needs to be prepared by having a secondary DNS and a backup resource of records in case an attack happens. In this paper author tells that Researchers and industry leaders should redefine and innovate new approach to address how security is thoroughly integrated in IoT cloud environment to preserve data confidentiality, integrity and authenticity. In fact, the number of cyber-attacks affecting the IoT ecosystem is increasing. A framework of distributed nature might play an important role to secure IoT data.

As in cryptanalysis, measurement of information leakage is the fundamental principle underlying the theoretical framework for robust watermarking security assessment presented in this paper [7]. A watermarking technique, even if it is robust, is not secure if the opponent can refine his knowledge on the presumably secret key while pieces of content are watermarked with the same key.

In this paper writer Alsubaei et al. discuss about some characteristics and some challenges of internet of medical things. Many healthcare providers are using internet of things technology to access their patient's data remotely to deal any kind of emergency [1]. IoMT layer also discussed in which each layer provides specific functionality and each of these functionalities possess a security and privacy issues, which are also, part of it. However, with these benefits, some of the security and other types of issues are also being arising like complexity and heterogeneity of different connected devices, Wireless sensor network security violations and breaches of authentication and authorization. In addition, there is a need for standards that regulate and mandate minimum security and privacy requirements for medical things. Due to the rapid evolution of technology and hacker skills, there might be new or unknown threats, features and framework of different nature that need to be considered in the future to overcome this issue.

Concerned study Shae et al. describes different applications in healthcare and their security challenges [8]. Wireless sensor network (WSNs) used in healthcare, automation of home, office and in other environment. Human wearable devices are also use on human body surface to examine the temperature, pulse oximeter, heart rate Blood pressure etc. Different challenges also discussed like resource scarcity, privacy and security issues. Prakash also designed an application scenarios for a nursing home, home care and in hospital [3].Concerned study showed the integration of blockchain and big data technology for the clinical data and health information records of Chinese Medicine University hospital and Asia University Hospital at Taiwan and Taiwan National Health Insurance Database Medical Data. Blockchain technology used for making the medical record more secure due to it distributed nature of blockchian. The resulted ecosystem provides the more accurate prevention of disease. The purposed system is not complete yet as it is undergoing at the Asia University, Taiwan. Various technology challenges are there. Blockchain is an anonymous hash value of user's public key. However, it was reported about 60% of the user Identity in the traditional blockchain, their real identities had been identified via the big data analysis across various data sets available in the Internet so it is required for the users to maintain its own identity anonymous.

Conventional healthcare systems do not allow patients to access and modify their data. If a patient switches from one healthcare provider to another then if anyone from his/her provider has a possibility to thief data [9]. There is another issue in conventional healthcare system to share patient's data securely from one provider to another even when a patient is also willing to allow the access to other provider. The incompatibility of conventional health applications stops the execution of secure patient-oriented read/write access control mechanisms to solve these common issues. Existing literature however provides little/no measures/guidelines for evaluating/creating block chain-based healthcare applications to avoid such issues however different set of evaluation metrics are described by using blockchain technology to overcome these issues. Appropriate evaluation metrics are missing here and there is not a proper way to validate the findings.

Tamizharasi et al. Gives the review some of the security considerations and challenges of IoT based E-Health systems [10]. Elements and effectiveness of Centralized and distributed architecture of IoT-based E-Health System are described. In performance aspect, distributed architecture supports speed-up and lack at scale up measures whereas cloud-based system is considered more efficient for large and complex EHR. Variety of access control algorithms such as DAC, MAC and Attribute based encryption techniques are discussed. The major drawback of the DAC method is that it is an all or nothing method. DAC method fails to provide the multi-level security which is the basic requirement of the IoT-based E-Health systems. The MAC model provide multi-level security and provides data access provision at user account and relation levels. It provides a high degree of data access protection and prevents illegal flow of information. However, the MAC model is too rigid, and it is applicable only to the limited environment. In CP-ABE the data access policy is attached to the ciphertext of the data content, and the user key comprises a set of attributes. This makes it computationally secure. However, the process of user attribute management and data access policy specification remains to be the major drawback of CP-ABE systems. The process of reduction of ciphertext length to the constant size and managing the meaningful attributes across the cloud computing environment is the most adopted solution to solve the drawbacks of the CP-ABE systems. So an appropriate selection of architecture elements and access control techniques provides better performance and security measures.

Bertino et al. discussed the key challenges in data security and privacy of IoT devices. Research directions are set for securing IoT data, including efficient and scalable encryption protocols, software protection techniques for small devices [11]. IoT systems are highly heterogeneous with respect to

communication medium and protocols, platforms, and devices. Writer told that most common IoT vulnerabilities arise because of the lack of adoption of well- known security techniques, such as encryption, authentication, access control and role-based access control. Reason for the lack of adoption may certainly be security unawareness by IT companies involved in the IoT space and bend-users. However, another reason is that existing security techniques, tools, and products may not be easily deployed to IoT devices and systems, for reasons such as the variety of hardware platforms and limited computing resources on many types of IoT devices.

state-of-art of lightweight cryptographic primitives which include lightweight block ciphers, hash function, stream ciphers, high performance system, and low resources device for IoT environment are discussed in details as IoT devices have to face different challenges in heterogeneous environment like power consumption of devices, limited battery, memory space, performance cost, and security in the Information Communication Technology (ICT) network [12]. Writer also told the reason for adopting new technology for IoT devices, which are Efficiency of end-to-end communications and Adoptability in low resources, smart devices. Symmetric and asymmetric algorithms are also discussed for encryption of data but these lightweight algorithms still do not give guarantee of security in real-time, execution time, power consumption and memory requirements. Symmetric algorithms lack of authentication whereas asymmetric suffers its larger key size and the consumptions of more memory. Elliptic curve cryptography (ECC) Compared to the RSA(asymmetric) algorithm is better because it a smaller key size. Writer also proposed a Hybrid Lightweight Algorithm (HLA), which is the combination of lightweight symmetry and lightweight asymmetric encryption algorithms for IoT devices. However, there are issues which needs to be tackle still related to the existing solution like block size and key size, new security attacks and its matrices.

Rabah et al. Discussed the increasing requirement of IoT security related to the characteristics of heterogeneity, resource constraints and dynamic environment [13]. According to writer heterogeneity problem is due to the absence of common security service for all IoT devices. Unified IoT security standards should be applied to for providing common securely service. Resource constraints is also a hurdle for providing secure cryptographic algorithms for which scalability has to be considered which means one have to design lightweight algorithms to that might not affect the efficiency of IoT devices. Moreover, some requirements and issues are considered in IoT environment on the following six layers: IoT network, Cloud, User, Attacker, Service and platform. Writer told that the existing researches do not cover overall security requirement for IoT environment. We need to analyze international standards related to the IoT security for interoperability among a Iot of diverse security platforms, devices and polices.

This paper reviews the new environment using HIoT, to identify the challenges for security and the impact of this on interoperability in the healthcare setting. Writer told that there are 70% of IoT devices who are found to have major security vulnerabilities which are due to the unencrypted network services and weak password requirements [14]. Regulatory medical device environment is one of the challenges of IoT security. The range of devices together with the necessity for trusted and reliable connection is critical to this technology uptake. Device diversity and interoperability is also a challenge for IoT security. Authentication and identity management should be there in the form of encryption of data in transit, and sufficient authorization and authentication measures of proper securing data. Other issues can also be addressed by using secure services (SOA modelling) and an end-to-end IoT service [15].

Proposed Methodology

The proposed healthcare system starts when IoMT wearable devices starts storing the patient's data. As said that proposed system is distributed nature so all the devices have their local databases to store their data. This is due to avoid from Denial of service attacks during data transmission which allows attackers to intercept data, and help them to obtain sensitive and valuable information about the patients. These Attackers also try to flood the healthcare system with traffic that is higher than the system capability which makes the healthcare system slow in responding to the user request and sometimes it lead to crash of the system and loss of the patients data. So having personal database of each device will minimize the chance of crashing the whole system as only concerned device/s will receive the particular request of its data. Response time is also increased as distributed system is managing the request load. Every patient having one of more devices have their unique ID which is stored in the patient mobile wallet. Doctor can access the patient device data by sending request to unique ID. Device level encryption is used to so that patient data could not be vulnerable to hackers during cloud transfer or synchronization with interconnected devices **(Figure 1).**

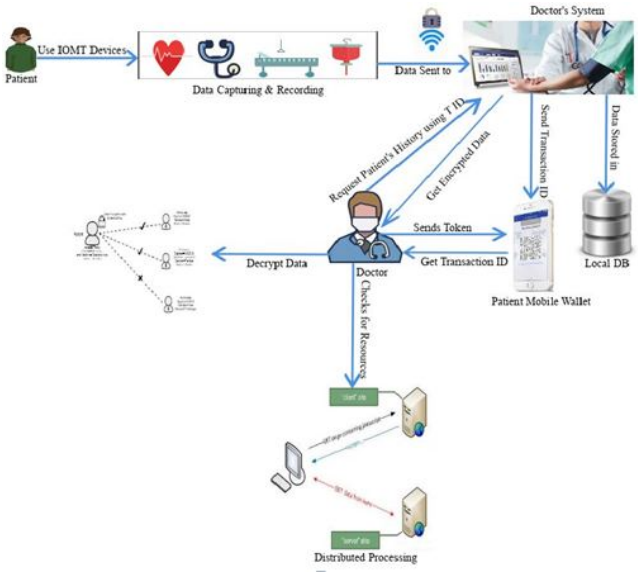

Figure 1: Architecture of proposed distributed system.

Our contributions

The major contribution of the proposed research work is listed as follows:

- First, a state of the art system architecture for the IoT based E-health systems is given in detail with a brief description of its architecture elements.
- Server level and device encryption applied in centralized and distributed (respectively) systems to show the difference between these two systems and to provide encrypted network service.
- Next, as a distributed nature a list of access control algorithms for IoT-based E-Health systems is provided and the most suitable one for the IoT based E-Health systems are suggested.

Component of the proposed architecture

As already mentioned that the proposed system is a distributed framework for security of IoT healthcare data So following are the main components of the whole architecture from data generation through different IoT wearable devices to data receiver at healthcare provider system.

- In distributed system, each node/device have its own database to store data locally. Therefore, Connectionis start up of the proposed distributed system through which doctor or other healthcare provider request for data using their IoT devices by sending token at the patient's healthcare device. There is a concept of patient mobile wallet, which is a repository containing transaction IDs for each block of data on daily/ weekly basis. So healthcare provider sends request for data using this Id in mobile wallet.
- healthcare provider uses this component to respond against the request generated on the network. If the responding node found the transaction Id valid by using which request is made, then in response healthcare data is shared with the requesting doctor.
- As already mentioned due to the resource constraint of IoT devices they use authentication algorithms according to their computing power. So When the request for the patient's history is made then the required data security format is also mentioned at the request time in which healthcare data is required. If the responding node is using same encryption technique to protect data format as the requesting node, then data is shared directly from the requesting device. But if there is a difference in the requesting and responding healthcare provider's cryptographic data format or there is no encryption algorithm is being used due to the extremely less computing power of device then the system searches in the nearby devices that can work with both the cryptographic data formats. So data is encrypted (required format) by some other high power computing device and then shared with the requesting node.
- Posting is end result in the form of required encrypted data securely. After encrypting the healthcare data in required cryptographic format in searching part, that system directly sends the data to the requesting node. There is a need to verify that the data is coming from an authentic node Results.

In our proposed architecture, different encryption techniques are used according to the IoT device resource constraint e.g. asymmetric encryption, Cipher-text policy attributes based encryption and to work with the low power devices, ECC (Elliptic Curve Cryptography) is used. As IoT devices are low power devices and ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC keys are much smaller than other encryption techniques like RSA keys. The strength of an ECC key is half the key size, so a 256-bit ECC key has 128 bits of strength. A similarly strong RSA key is 3,076 bits long. As key size is much smaller than other

cryptographic techniques therefore ECC is suitable for secure data transmission among low power IoT devices. Our contribution to the proposed distributed architecture is that we are using hybrid encryption technique of ECC with attributes, the user has to provide the private key as well as the user attributes to get the data. The distribution of devices based on encryption technique is shown in the table below. As IoT devices are low power devices so most of the devices are using ECC technique as it has low key size and works well for low power devices. But as we want to work with the low power devices but also want the security to be strong therefore as our contribution we are adding attributes with the ECC to get the decrypted data. As shown in the **Table 1** below that number of devices using ECC + ATTRIBUTES is less than the ECC devices but it will be increase in the near future to work with it.

Table 1: Comparison to security properties.

Properties	Symmetric	Asymmetric	CP-ABE	ECC	ECC +Attributes
Security	Low	Medium	High	High	High
Privacy	Low	Medium	High	High	High
Key size	Large	Large	Large	Small	SmalL
Multi-Level Security	No	Yes	Yes	Yes	Yes
Encryption On Devices	10%	10%	20%	35 %	25%

Results and Discussion

It is observed that 70% of IoT healthcare devices found to have serious security vulnerabilities, including using unencrypted network services and weak passwords so proposed system using So security layer implemented in proposed system to facilitate additional layers of encryption on device level that enforce the privacy of content embedded within transaction data. In order to enable data sharing across healthcare systems, we developed a purpose-built solution based on patient data privacy and security requirements that leverage a collection of strong encryption algorithms using distributed nature to enable healthcare based data secret sharing. Proposed system also

suspends the Denial of Service attack as all IoT devices have their own local database to minimize load on server. Resource constraint issue of IoT devices also handled by providing authentication facility from neighbouring high computing power devices. In **Figure 2** Results shown in previous section also reveals the effectiveness of the proposed system on both security and efficiency point of view.

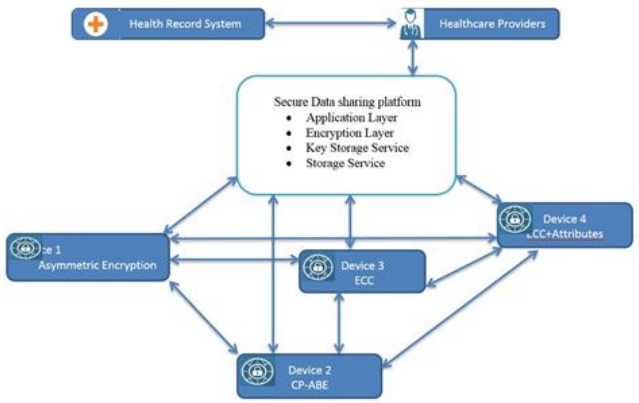

Figure 2. Illustration of the system Architecture of Distributed Solution.

Conclusion and Future Work

Concerned paper proposed a suitable architectures and access control techniques for the Distributed IoT healthcare environment clearly with its functionalities. Security layer implemented in proposed system to facilitate additional layers of encryption on device level that enforce the privacy of content embedded within transaction data. To face the challenge of IoT device resource constraint different cryptographic algorithms are implemented according to the computing power of IoT wearable devices. Research has proofed that Eliptive Curve Cryptography (ECC) is better technique to work with low power devices as it uses small key size. We purposefully proposed the usage of ECC with attributes as an additional metric to improve the security level. Effectiveness of proposed system also accomplished by designing Denial of Service attack on ten different devices to show the better average response time of the system.

References

1. Alsubaei F, Abuhussein A, Shiva S (2017) Security and privacy in the internet of medical things: Taxonomy and risk assessment. In: Proc. - 2017 IEEE 42nd Conf. Local Comput. Networks Work. LCN Work 6 : 112–120.
2. Kumar BV, Ramaswami M, Swathika P (2017) internet of medical things (IoMT) using hybrid security and near field communication (NFC) technology. Int J Comput Appl 174: 37-40.
3. Prakash S (2016) An overview of healthcare perspective based security issues in wireless sensor networks. In: 2016 3rd International Conference on Computing for Sustainable Global Development IEEE: 870-875.
4. Alasmari S, Anwar M (2016) Security and privacy challenges in IOT-based health cloud. In: 2016 International Conference on Computational Science and Computational Intelligence IEEE: 198-201.
5. Mehta D, Sera O, Kim YG (2017) Internet of medical things note on futuristic healthcare. Security Requirements Analysis for the IoT.
6. Hossain MS, Muhammad G (2016) Cloud-assisted industrial internet of things (Iiot)–enabled framework for health monitoring. Computer Networks 101:192-202.
7. Cayre F, Fontaine C, Furon T (2005) Watermarking security: theory and practice. IEEE Transactions on Signal Processing 53:3976-3987.
8. Shae Z, Tsai JJ (2017) On the design of a blockchain platform for clinical trial and precision medicine. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) IEEE: 1972-1980.
9. Zhang P, Walker MA, White J, Schmidt DC, Lenz G (2017) Metrics for assessing blockchain-based healthcare decentralized apps. In: 2017 IEEE 19th International Conference on e-Health Networking. Applications and Services IEEE: 1-4.
10. Tamizharasi GS, Sultanah HP, Balamurugan B (2017) IoT-based E-health system security: A vision archictecture elements and future directions. In: 2017 International conference of Electronics, Communication and Aerospace Technology ICECA IEEE. 2: 655-661.
11. Bertino, Elisa, Lafayette W (2016) Data security and privacy in the IoT. Big Data in Internet of Things (IoT) Key Trends, Opportunities and Market Forecasts 2015 –2020: 18-20.
12. Singh S, Sharma PK, Moon SY, Park JH (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Amb Intel Hum Comp 1-8.
13. Rabah K (2017) Challenges and opportunities for blockchain powered healthcare systems: A review. Mara Res J Med Health Sci 1:45-52.
14. Al Alkeem E, Shehada D, Yeun CY, Zemerly MJ, Hu J (2017) New secure healthcare system using cloud of things. Cluster Computing 20: 2211-2229.
15. Williams PA, Mc Cauley V (2016) Always connected: The security challenges of the healthcare Internet of Things. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) IEEE: 30-35.