Blended Cryptography for Secured Data Transfer in Medical IoT Devices

Revanesh. M
Dept. of Electronics and Communication
PES College of Engineering
Mandya, India

Dr. V. Sridar
Professor, Dept. of Electronics and Communication
PES College of Engineering
Mandya, India

***Abstract*—To make the best use of the vast potential opportunities that accompanies medical IoT sensor devices, security and privacy measures are expected to be inculcated as fundamental requirement within these systems. Although cryptography proves to be a promising solution for data breach problem, there is always an inconclusive debate between the usages of symmetric encryption schemes which provides reduced computation overhead and asymmetric encryption schemes that delivers better authentication in IoT devices. This research paper focuses on a brief analysis of various existing symmetric and asymmetric lightweight algorithms for IoT. Using simulation tests, we provide important analysis and considerations on practical feasibility of these cryptographic algorithms in IoTs built using sensor networks to help designers predict security performance under a set of constraints, we also propose a new methodology which blends the usage of both symmetric and asymmetric encryption scheme for enhanced data transfer in health care related IoT devices.**

Keywords—Biomedical; Internet of Things; cryptography; symmetric encryption; asymmetric encryption

I. INTRODUCTION

With the rapid growth in the fields of wireless communication and medical sensors, Medical IoT now starts moving towards a reliable future technology rather than a scientific fiction. Medical IoT devices have also made the health care systems more patient centric rather hospital centric, by making vital data of patients available anywhere and anytime to anyone. Most of the time these vital data obtained from sensors or wearables attached to patient are usually transferred wirelessly using a channel which has free access to everyone, with zero or minimum concern about security and privacy issues.

Forbes report a number of security breaches related to health care [1] which has accounted for a loss of more than 112 million medical records by various incidents like Hacking, loss etc., in which sensitive, protected or confidential data is duplicated, accessed, stolen or used by an individual or group of unauthorized people. Information contained in health care records is always proved to have longer value and is rich enough for identity theft.

Despite the vast range of potential applications, there is a huge difference between the security requirements [2]-[4] that the medical IoT poses and the existing security mechanisms. As the numbers of connected medical devices are multiplying, it becomes inevitable to electronically process the huge amount of data handled by these devices which demands the research community to develop security algorithms tailored to satisfy the requirements of resources constrained Medical IoT devices.

To make the best use of this vast potential opportunities that accompanies IoT, security and privacy measures are expected to be inculcated within these systems, neglecting which can outbreak serious data breaches and other cyber security nightmares. Although cryptography proves to be a promising solution for data breach problems, implementation of conventional cryptography on resource constrained sensor devices aggravates the security challenges [5], [6] and demands for light weight cryptography techniques which reduces the computational overhead without bargaining on the security.

In this paper we make an effort to identify some of the security requirements of Medical IoT devices and see how they are addressed by existing proposed systems. The rest of the paper is structured as follows:

In Section II, we elaborate the security requirements in a biomedical sensor networks while in Section III, we review some of the popular proposed Bio medical IoT Frameworks and discuss the security requirements of those networks. In Section IV, we review some popular cryptography algorithms, and in Section V, we describe a new blended security methodology suitable for biomedical IoT network which is flexible enough to account different levels of security requirements in the network and discuss its advantage over regular data transfer approaches and conclude with the future scope of the project.

II. SECURITY REQUIREMENTS IN BIOMEDICAL IOT NETWORKS

Security is always considered to be one of the key requirements of any modern day technology. Research community and product developers have their own perspective of security and hence it is usually defined in many ways. In more traditional way, security can be defined as measures taken to increase the safety of IoT network. In this section, we describe the key security requirements [7]-[10] in IoT based healthcare system.

A. Data Confidentiality

Like any other wireless systems data confidentiality is one of the prime concerns in IoT based Health care systems. It is required to protect the patient's vital data from disclosure to any other person. A Hacker who is listening to this network

can easily eavesdrop on the communication, which can cause serious issues not only for the patient but also to the insurance companies and hospitals as the data collected here can be used for many illegal activities which can affect the society.

B. Authentication

Authentication refers to the security measures used to make sure only an authentic user can have access to the network or medical data gathered using Health care IoT devices, failing which an adversary can cause critical damages to the data records, which can result in health insurance Frauds (i.e., an act of deceiving or misrepresenting information that results in health care benefits to an individual or group).

C. Integrity

Data integrity refers to an act of security concern, where the data is reliably transmitted along the length and breadth of network without modification or loss. It is always of prime importance to maintain data integrity in a health care IoT neglecting which can cause serious irreversible damages related to DRUG FRAUD (an act where a bad dosage quantity of drugs are given to patient which can cause death) or even Insurance Fraud, etc.

D. Data Freshness

It is an act which guarantees that the data transmitted in the network are recent and fresh data rather than an old repeated data sent by an adversary. To ensure data Freshness time stamp can be attached to each data packet before they are sent.

So it is of importance to note that any security protocol designed for IoT should always address Access control, data integrity and data confidentiality as primary requirements. All of the above mentioned requirements can be addressed by inculcating Cryptography in the network.

III. LITERATURE SURVEY AND MOTIVATION

Most of the recent work carried out in the field of biomedical IoT shows that it is possible to continuously monitor health condition of a patient through a set of sensors attached to patients.

CodeBlue [11] which is a popular project carried out at Harvard Sensor Network Lab, in which series of bio sensors are placed on patient's body to record vital parameters and data collected from these sensors are transmitted to end user device such as PDAs, Laptops and personal computer of experts for monitoring purpose. However the authors here lists out encryption algorithm requirement as one of the top most priority challenge along with various other research challenges which are expected to be addressed to achieve the level of robustness required for medical IoT.

UbiMon (Ubiquitous monitoring environment for wearable and implantable sensors) [12] is a BSN (Body Sensor Network) architecture composed of wearable and implantable sensors using an ad hoc network developed at Imperial college, London. The aim of the project is to provide continuous monitoring of an individual's physiological states and capture transient as well as life threatening abnormalities that can be detected and predicted. Although Ng et al. proposed and demonstrated the UbiMon architecture. The authors also accepted that without considering security for such applications they are often vulnerable to security attacks.

Personal ambient monitoring (PAM) project [13] for mental health monitoring is a project which aims to monitor the activity signatures of patients with bipolar disorder (BP) using body and environmental sensors, mobile phones, and personal computers. This is considered to be the first attempt to obtain activity signatures from the mentally ill patient using worn and environmental sensors networks. Although, authors blaze a new research trail for mental illness monitoring, they focused mainly on reliability and acceptability issues without much concerns patient privacy and data confidentiality which is an imperative requirement for such applications.

The research work [14] carried out at university of Virginia developed a patient monitoring system in assisted living and home environment scenarios. Although, the authors have facilitated data security Wood *et al.* pointed out that it is susceptible to adversarial confidentiality attack and suggests the usage of Cryptography algorithms for better security.

In 2006, Chakravorty [15] developed a mobile health care project called MobiCare which provides a wide-area mobile patient monitoring system that facilitates continuous and timely monitoring of patients physiological status where in author acknowledges the requirement of proper encryption algorithms to make the health care monitoring systems more reliable.

Recently the works carried out in many different universities across the globe [16], [17] et al. elaborates the requirement of proper encryption standard for making the biomedical health monitoring system more robust in nature and suitable for real time application.

From the literature survey carried out it is clear that most of the healthcare monitoring projects which enables monitoring of a person under critical or hospitalized environment emphasizes the need for security and privacy of the data transmitted through the network but only handful of them implement it and the ones which implement it still are facing problems related to concluding which encryption algorithm can be used to solve the issues related to privacy in healthcare applications, which is a mandatory procedure according to government laws in many countries [18].

IV. CRPYTOGRAPHY

Cryptography not only guarantees Data security and data privacy of a network but also increases the reliability of any network to which it is applied, but because of the constraints that IoT devices introduce, such as limited processing power, limited memory, traditional cryptography algorithms cannot be transferred directly onto these devices. Therefore, traditional cryptography algorithms have been tailored in such a fashion that they suit the requirements of Resource constrained devices while still maintaining the required security level, which are popularly known as lightweight Cryptography algorithms. Some of the Existing Symmetric lightweight algorithms [20]-[23] for IoT scenario along with their key sizes are given in Table 1.

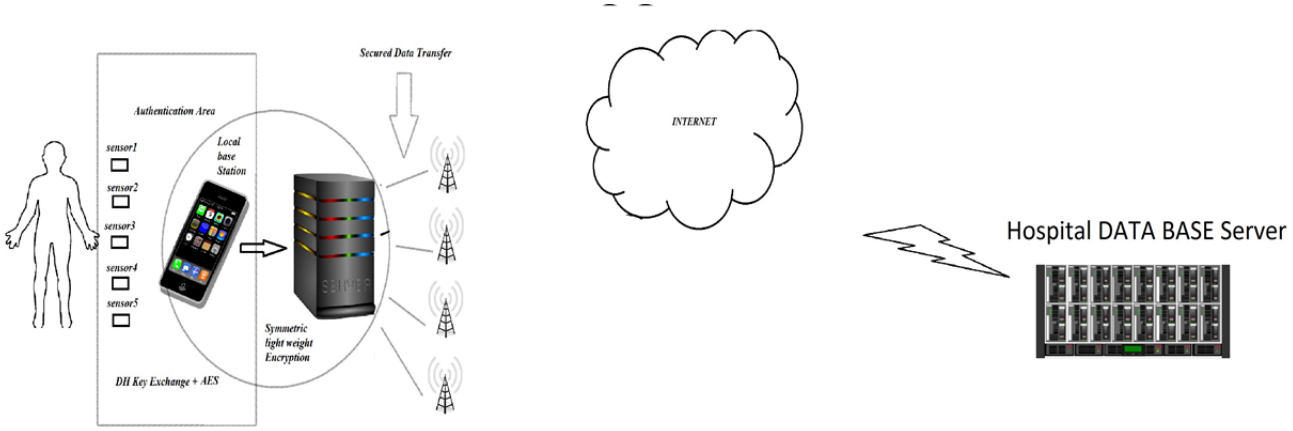

Fig. 1. IoT framework with blended encryption.

TABLE I. COMPARISON OF LIGHT WEIGHT ENCRYPTION ALGORITHM

Name of the symmetric algorithm	***Key size bits***	***No of rounds***	***Block Size bits***
AES	128	10	128
HIGHT	128	32	64
3 DES	112	48	64
BLOWFISH	32-448	16	64
RC5	16(Variable)	20(minimum)	32(minimum)

V. PROPOSED METHODOLOGY

The new methodology proposed for medical IoT composes of two-fold security measures:

1) Authentication of Sensors or medical related Physical devices by Local Base station.

2) Confidential transfer of diffused data obtained from Local Base station to servers.

The algorithm is executed in the following steps:

Step 1: Authenticate every Physical device using Diffie-Hellman (DH) key exchange algorithm and AES (advanced Encryption Standard) to make sure that only authenticated sensor nodes participate in the data collection process. Once a secured network is established it is usually very difficult for adversaries to participate in the data exchange process.

Step 2: Next step is to make sure that any adversary in between cannot eavesdrop on the information transmitted from bio medical sensor node end to Local Base station. This is done using symmetric lightweight cryptographic algorithms like RC5 which not only prevents eaves dropping but also creates an extra layer of security.

Data from authentic sensor node (D_s)	Time Stamp (Ts)

Fig. 2. Data from base station.

Step 3: Once the data reaches home server via Local Base station or processing unit, this assembled data is then transmitted to the hospital server for feedback from experts.

Fig. 1 shows the framework where in a patient is monitored with number of similar sensing devices to monitor vital parameters from the body using the proposed methodology.

First as an initial step, various light weight cryptography techniques are analyzed for their usage in the proposed methodology by evaluating their performance in terms of various parameters like key size and execution time by providing them with different sizes of data. The comparison results are shown in Table 2. The results clearly revealed that for varying data sizes RC5 and AES encryption algorithm have the same encryption time, which emphasizes that any of these can be used for transferring data from Local Base station to the server. Base station also adds a time stamp to the Data being transmitted as shown in Fig. 2.

The sensor node authentication is a prime requirement to meet the expected data privacy in medical IoT. Various cryptography techniques (AES, RC5 and 3-DES) along with Diffie-Hellman Key exchange [19] are first analyzed to choose the best possible solution for IoT usage, from the experimental results it was observed that AES along with DH Key exchange proves to be a promising solution for medical IoT devices with comparatively faster data transfer rate(less delay) as shown in Table 2 and also offers an enhanced network lifetime (due to reduced complex operations). So Every Biomedical sensor nodes used are authenticated using a combination of Diffie-Hellman key exchange with AES.

TABLE II. COMPARISON OF LIGHT WEIGHT ENCRYPTION ALGORITHM

Input datasize in KB	***Algorithms + DH KEY EXCHANGE***			
	AES-128 In ms	***3DES-112 In ms***	***RC4-40 (In ms)***	***RC5-128 (In ms)***
150	60	89	97	63
200	90	126	135	95
300	120	150	180	122
500	156	179	196	160
1000	389	562	498	396
1500	792	1123	623	790

Once the nodes are authenticated, the data collected from each node with an extra 4 bit of data (time stamp) as shown in Fig. 3 is transmitted to the local base station where the data from different sensors are assembled and an extra layer of security using simple symmetric cryptography (SC) techniques (by using Pseudo random generator with Key(K)) is added on the assembled data and then transferred to the home server, which transfers the encrypted data from home server network to hospital or required place for the expert feedback via internet.

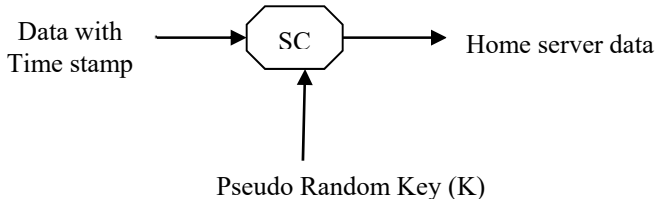

Fig. 3. Data assembling at home server.

The performance of the proposed methodology is compared with regular IoT data transfer which uses public key cryptography on a channel with AWGN. Fig. 4 shows the results of comparison of traditional cryptography usage for Medical IoT network with proposed methodology and the following observations were made.

The network with DH Key exchange algorithm along with AES provides enhanced transfer of secured data even in noisy conditions when compared to other traditional networks which employ a single encryption standard, which not only protects the data from hackers as in conventional cryptography mechanisms but also ensures data integrity and data freshness by using asymmetric DH key exchange and by attaching a time stamp to the data before transmission, but the enhanced data transfer comes with an extra cost of processing time which is comparatively 2/3 times higher than the public symmetric key exchange schemes for a constant signal to noise ratio over an AWGN channel as shown in Fig. 5.

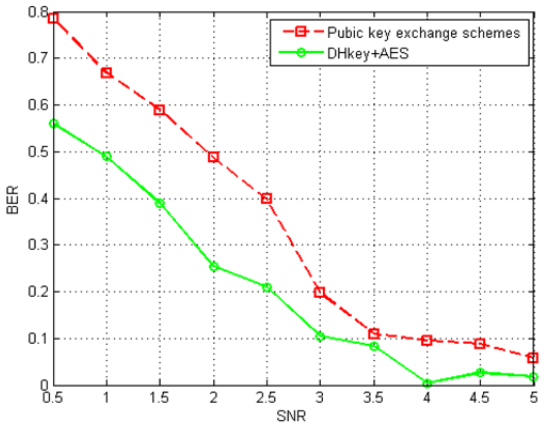

Fig. 4. BER of Networks at different SNR.

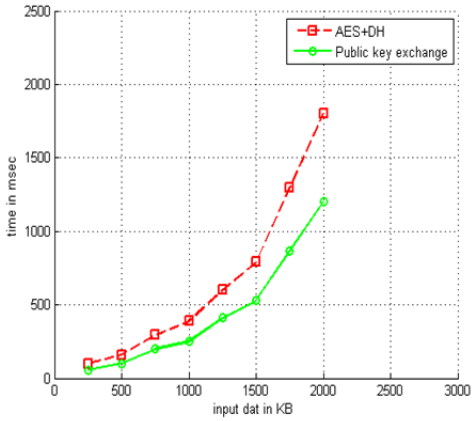

Fig. 5. Execution time comparision of public key exchnage and DH Key+AES.

VI. CONCLUSION

In this paper we consider the problem of delivering collected data from IoT based biomedical sensor nodes to the hospital server and proposed an efficient manner to meet the security level required to maintain the data integrity using blended use of cryptographic techniques. We also studied the trade-off between different symmetric techniques in terms of execution time and proposed for an implementation of new framework that uses Asymmetric Encryption techniques at the node end for authentication and symmetric encryption technique at base station for data transfers, to maintain data privacy. Although there is an increase in the execution time the

increase is due to the authentication process involved, which not only restricts unauthenticated users participation but also increases the data packet delivery ratio even in noisy environment like AWGN channel there by reducing the ARQ (Automatic Repeat Request). Thus the extra overhead introduced in terms of execution time at the initial stages for authentication can be considered as a tradeoff for increased lifetime of the network.

Also by using the proposed scheme in IoT devices not only the man in the middle attack (intruder attack) can be overcome, but also by integrating extra time stamp with the data to be processed the data freshness can be ensured. Although simulation results show improvement in error rate probability but the practicality of the results is expected to be tested on real time hardware.

REFERENCES

[1] Dan Munro "Data Breaches In Healthcare Totaled Over 112 Million Records In 2015" Availble : http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#7bb4e8917fd5.

[2] W. Maisel, "Safety Issues Involving Medical Devices," J. Am. Medical Assoc., vol. 294, no. 8, 2005, pp. 955–958.

[3] D. Halperin, "Security and Privacy for Implantable Medical Devices", IEEE Pervasive Comp., vol. 7, no. 1, pp. 30-39, Jan. 2008.

[4] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1,pp. 55–91, 2012.

[5] P. Ganesan, R. Venugopalan, and P. Peddabachagari, "Analyzing and modelling encryption overhead for sensor network nodes," ACM in Proceedings of WSNA'03, pp. 151-159, Sep. 2003.

[6] C. T. R. Hager, S. F. Midkiff, J. M. Park, and T. L. Martin, "Performance and energy efficiency of block ciphers in personal digital assistants," Third IEEE International Conference on Pervasive Computing and Communications, pp. 127-136, Mar. 8-12, 2005.

[7] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, ―"Security challenges in the IP-based Internet of Things"‖ *Wirel. Pers. Commun.*, vol. 61, no. 3, pp. 527–542, 2011.

[8] R. H. Weber, ―Internet of Things – "New security and privacy challenges"‖ *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[9] P. Gope T.Hwang "BSN Care: A Secure IoT-Based Modern Healthcare system Using Body Sensor Network" IEEE Sensor Journal, vol-16,No5 pp. 1368-1376, March 2016.

[10] K. Lorincz et al., "Sensor networks for emergency response: Challenges and opportunities," IEEE Pervasive Comput., vol. 3, no. 4, pp. 16–23, Oct./Dec. 2004.

[11] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "CodeBlue: An ad hoc sensor network infrastructure for emergency medical care," in Proc. MobiSys Workshop Appl. Mobile Embedded Syst. (WAMES), Boston, MA, USA, Jun. 2004, pp. 1–8.

[12] J. W. P. Ng et al., "Ubiquitous monitoring environment for wearableand implantable sensors (UbiMon)," in Proc. 6th Int. Conf. Ubiquitous Comput. (UbiComp), Nottingham, U.K., Sep. 2004, pp. 1–2.

[13] Blum J.M., Magill E.H. The Design and Evaluation of Personalised Ambient Mental Health Monitors. Proceedings of IEEE CCNC 2010; Las Vegas, NV, USA. 9–12 January 2010.

[14] A. Wood *et al.*, "ALARM-NET: Wireless sensor networks for assistedliving and residential monitoring," Dept. Comput. Sci., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep. CS-2006-01, 2006.

[15] R. Chakravorty, "A programmable service architecture for mobile medicalcare," in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshop (PERSOMW), Pisa, Italy, Mar. 2006, pp. 531–536.

[16] Ko J., Lim J.H., Chen Y., Musaloiu-E. R., Terzis A., Masson G.M. "MEDiSN: Medical Emergency Detection in Sensor Network"s. ACM Trans. Embed. Comput. Syst. 2010;10:1–29.

[17] Ganti R.K., Jayachandran P., Abdelzaher T.F., Stankovic J.A. SATIRE: "A Software Architecture for Smart AtTIRE". Proceedings of MobiSys'06; Uppsala, Sweden. 19–22 June 2006; pp. 110–123.

[18] Office for Civil Rights, United State Department of Health and Human Services Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information. Availableonline:http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.

[19] P.Joshi, M.Verma, Verma "Secure Authentication Approach Using Diffie-Hellman Key Exchange Algorithm for WSN": IEEE Int. Conf. ICCICT 2015. Dec.2015 :pp527-531.

[20] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz: "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs" :Proceedings of IACR/2004/ Available :https://www.iacr.org/archive/ches2004/31560117/31560117.pdf.

[21] Isha and Ashish "Analysis of Lightweight Cryptographic Solutions forInternet of Things" IJST Journal.Vol.9, July 2016.

[22] X.Yao, Z.Chen,Ye "A lightweight attribute-based encryption scheme for theInternet of Things" Elsevier journal on Future Generation Computer Systems 49 (2015) 104–112.

[23] T. Eisenbarth S.Kumar *et al.* "A Survey of LightweightCryptography Implementations": IEEE Design & Test of Computers (Volume: 24, Issue: 6, Nov.-Dec. 2007) pp- 522-533.