RESEARCH ARTICLE OPEN ACCESS

Secured Data Communication Protocol Based Modern Patient Health Monitoring System

K. Dinesh kumar[1] ,S. Steve revanth[2] ,R. Subin[3] ,Antony Robert[4]

[1, 2, 3, U.G]. Students, Dept. of CSE, Alpha College of Engineering, Chennai.
[4]Asst.prof. Dept. of CSE, Alpha College of Engineering, Chennai.

Abstract:

The body area network (BAN) technology is one of the core technologies of IOT developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight sensor nodes. However, the development of this new technology in healthcare applications without considering security makes patient privacy vulnerable. In this paper, at first, we highlight the major security requirements in BSN-based modern healthcare system. Subsequently, we propose a secure IoT-based healthcare system using BSN, called BSN-Care, which can efficiently accomplish those Requirements.

Keywords — ***Body Area Network (BAN); Attribute Based Encryption (ABE); Internet of Things (IOT);***

I. INTRODUCTION

The Mobile-Health system has been envisioned as a promising approach to improving healthcare Quality and save lives in the aging society. In Health Systems, the Personal Health Information (PHI) is Collected by Body Area Network (BAN) and aggregated by A. Zhang and L. Wang are with the Key Lab of Broadband Wireless. Communication and Sensor Network Technology. Then the data is sent to the healthcare center. Via cellular networks. With the increasing popularity of Mobile healthcare, the medical data sent to base stations may Aggravate the already over-burden cellular networks. Fortunately Device-to-Device (D2D) communications are proposed To be an advantageous solution to meet with the explosive Demanding of spectrum because they can be operated on the Same time/frequency resources over short distances . Consequently, we propose to transmit the PHI data through D2D communications in M-Health systems in this paper. However, due to the intrinsically open nature of wireless Communications and dynamics of cellular networks, D2D Communications are vulnerable to security attacks such as Eavesdropping, fake message, privacy violation, etc. Currently, Security for M-Health systems has attracted extensive attentions. Most of these works mainly focus on either Anonymous authentication or privacy-preserving issues while ignoring the security during data transmission. Lin *et al* Firstly consider this problem by proposing a strong privacy preserving Scheme against global eavesdropping for health Systems, followed by These are pioneer works on Security-aware data transmission for M-Health systems while They don't take into account the D2D-assist data transmission Scenarios .Actually, security-aware D2D-assist PHI transmission for M-Health systems is challenging due to the privacy sensitive Characteristics of PHI data and the insecure D2D transmission. Specifically, the protocol design should consider the following Issues: if) How to guarantee the PHI not to be accessed by the Relays while the relays are able to judge whether the data is Altered by attackers? ii) How to achieve mutual authentication between the source client of the data and its intended physician without interaction? iii) The proposed protocol should be light Weigh in the sense that the mobile terminals have energy and Storage constraints, i.e., the computational and communication Cost should be low. The protocol should be robust enough to face the threat when part of the keys are exposed, i.e., the PHI remains secure even if part of the keys are disclosed. In order to address the above issues, we use certificate less Public key cryptography (CLPKC) to achieve the designed Security objectives. In CLPKC, the users' private key is not generated by the Key Generator Center (KGC) alone but a Combination of the contributions of the KGC and the user. The KGC does not know the user's private key but can authenticate its public key. In this way, the key escrow problem of CLPKC avoids the problem of certificate revocation, storage and distribution in certificate-based public key cryptography. Generally, the CLPKC has three techniques, i.e., certificate less signature, certificate less encryption, and certificate less signcryption. The three techniques are usually realized by three different algorithms and are applicable in different application scenarios.

In order to adaptively work as a signcryption scheme, a signature scheme, or an encryption scheme with only one algorithm, a certificate less generalized signcryption (CLGSC) Scheme is put forward by Jim *et al* in [14]. Later, the authors in propose more efficient CLGSC scheme. However, all the existing CLGSC schemes are realized with pairing operations, Which is time consuming and has low computational efficiency. Motivated by the above, we propose a new CLGSC scheme which is low in time consumption cost and proven to be secure in confidentiality and enforceability. The new CLGSC algorithm can operate on three modes signcryption mode, signature mode, or encryption mode adaptively. We use CLGSC to design a light-weight and robust security-aware (LRSA) D2D-assist data transmission protocol for M-Health systems.

Firstly, the PHI data is encapsulated with signcryption mode and the source's identity is encrypted with the encryption mode by the source client, thus achieving data confidentiality and integrity, mutual authentication and contextual privacy. In addition, a session key is introduced in the signcryption algorithm to enhance the security strength. And the session key is updated by a secure hash function at the end of each transmission session to achieve forward security. Moreover, the source client and all the relays sign on the encrypted data to guarantee data integrity. Notably, the proposed LRSA protocol can also achieve anonymity and unlink ability by using the pseudo identity and a random number in the cipher text of the identity. In summary, our contributions are threefold. • We propose a new efficient certificate less generalized signcryption (CLGSC) scheme. The proposed CLGSC is built based on Elliptic Curved Discrete Logarithm Problem (ECDLP) and implemented without pairing. It has the lowest computational cost comparing with the existing CLGSC schemes. Moreover, it is proven to achieve confidentiality and enforceability in the random oracle model (ROM) under the Discrete Logarithm Problem (DLP) and CDHP (Computational Diffie-Hellman Problem) assumption. • We design a lightweight and robust security-aware (LRSA) D2D-assist data transmission protocol for M-Health systems based on the proposed CLGSC scheme. LRSA achieves data confidentiality and integrity, mutual authentication and contextual privacy by using the proposed CLGSC scheme. Furthermore, anonymity and unlink ability are simultaneously realized by using the pseudo identity and choosing different random numbers at different sessions. Additionally, LRSA has the characteristics of forward security with hash chain of the session key. • We analyze security properties of the proposed LRSA and compare it with the other protocols in terms of data confidentiality and integrity, mutual authentication, anonymity, unlink ability, forward security, and contextual privacy. Moreover, the computational overhead and Communication overhead are also compared between our proposed CLGSC algorithm and the other certificate less generalized signcryption schemes. The remainder of the paper is organized as follows. An overview on security in M-Health systems and certificate less public key cryptography is conducted in Section II. The system model is presented in Section III, followed by the preliminaries in Section IV. In Section V, the new CLGSC scheme is formed and proved secure in details. Section VI describes the proposed LRSA scheme and Section VII analyzes its security properties. In Section VIII, the performances of the proposed scheme are evaluated and compared with other schemes in terms of computational overhead and communication overhead. Finally, Section IX concludes this work.

II. RELATED WORK

Here we are implemented the new technology based on android system. Here, the patient status is automatically transferred to the mobile application. We implement attribute based Encryption technique for data security , Attribute based Encryption means Key generator generate encryption key based on Requested Authority Example Doctor, Nurse, Relative .can view full patient information if Request Authority is Doctor . Others cannot view full patient information but some cases, the data produced may be requested by authorized person like doctor, he can monitor and he can able to suggest the prescription or medicine to the patient. But others, like nurse or a relatives requested for monitoring, we eliminate the trust we put on the data sink by encrypting the stored data at the data sink. Thus the data sink itself has no access to the original data, so they can only view the data's

III. MODELS AND GOALS

A. System model

We consider an M-Health system consisting of three entities: Network manager (NM), WBAN clients, and medical service providers, as shown in Fig.1 *Network manager (NM).* NM is a powerful entity in charge of the whole system, e.g., initializing the system, membership
Management. In the proposed scheme, the NM also works as the key generation center. As the NM may be acted by the M-health center or a commercial organization, it can't be fully trusted. Consequently, the NM only generates partial private key for the registers to avoid the key escrow problem and is prohibited to access the patient health information. *WBAN clients*. The WBAN client is a medical user equipped with personal BAN and a mobile phone. The BAN consists of many body sensors such as blood pressure, oxygen saturation, temperature sensor, and so on. All the data sensed by the devices formulates the PHI, which is reported to the mobile phone. Note that mobile phone is a key component of the client as it processes PHI and sends the data to the NM for reaching the corresponding physician. Different from the in-bed patient at home or hospital, the WBAN clients are mobile users in our model, i.e., walking outside. The WBAN clients have to register to the NM for joining the M-health system before enjoying the medical service. *Medical service providers*. Medical service providers, such As the physician, clinic or hospital, provide physician consultation or medical services to the clients. They also need to be preloaded with the system parameters and register to the NM before they serve for the clients. In our model, we assume that the physicians take the role of medical service providers. We assume that at session t, the WBAN client S wants to report his PHI to the physician $H1$ while it is unable to reach the NM directly. So it searches other clients for help relaying the data. We assume that a reliable routing from the source client S to the NM has been established in our system model2, as shown in Fig. 1. The n clients formulate the relay set, denoted Here, $R1$ denotes the first relay receiving the data from the source, and Rn denotes the last relay which sends the data to the NM. Upon receiving the data from the relay Rn, the NM distributes the data to the intended physician.

B. Threat model and design goals

Threat model. As the PHI data passes through the relays
And NM before arriving at the physician, it faces the threat
Of revealing the source's private information. Specifically, the relays or eavesdroppers may disclose the health status of the source client from the PHI if the PHI is not confidential, which is called content oriented privacy. Even if the PHI is confidential to them, the relays or the eavesdroppers may deduce the source's disease once they find the intended physician of the client. On the other hand, as the NM delivers the data to the intended physician, he may find out the WBAN client's health information if he knows the source of the data. This privacy of the data source or destination is called contextual privacy. Moreover, semi-trustable NM may also

access the client's PHI or impersonate the clients and physicians for commercial benefits. Some malicious attackers may modify or fabricate the data for their own purposes. *Security objectives*. Based on the above system model and potential threats, the design goals of our scheme are as follows:

1) *Data confidentiality and integrity*. Data confidentiality
Protects PHI from revealing the source's privacy-sensitive
Information while data integrity ensures that the message is not altered during the transmission.
2) *Mutual authentication*.
The WBAN client and the physician can authenticate each
Other to guarantee that the data comes from the claimed source and arrives at the intended destination.
3) *Anonymity*. The real identity of the WBAN clients should be confidential to anyone (including the NM) except the intended physician.
4) *Unlink ability*.
The transmissions of any two sessions should not be
Linked to the same source WBAN clients.
5) *Forward security*.
If the full private key of the entity in the current session is
Exposed, the transmission protected by the previous session key remains secure.
6) *Contextual privacy*. The eavesdroppers
Or entities in the system, i.e., relays and NM, don't have the ability to link the source and the destination of the data if they don't collude. The following modules are

A) Sensor Interface:

WBAN is rapidly growing technology, in our project we used temperature, pressure, heartbeat sensors, these sensors are embedded in human body and synchronized with our mobile application. We have Heart Beat Sensor to monitor the heart beat and will notify in case of emergency.

B) Application interface:

In this module we create android application for receive data from sensor network, for energy efficient communication we implement Bluetooth network , WBAN sensors synchronized with android application, from android application data's are forwarded to main server. It analysis then stored in database.

C) Data analysis:

This module sensor data's are analyzed by Data analyst, if data value is normal that is encrypted by AES algorithm then stored in database user can view our data from our profile. If data values are abnormal; notifications are send to doctor, nurse, relative.

D) Key generator:

Key generator are server jobs of the server is generate key based on user request , it generate attribute based encryption key , access privilege based on this key , doctor can view and update or remove prescription and histories . But nurse can only view patient data; relative can only view patient current location and sensor values.

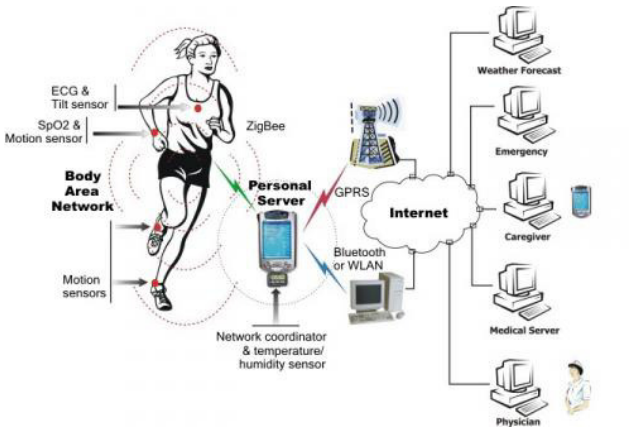

Fig 1.Proposed System Architecture

A generalized signcryption scheme can adaptively work a as signcryption scheme, a signature scheme, or an encryption scheme within one single algorithm, which is suitable for storage-constrained applications. The users may perform the algorithm according to the security requirements in different environments. As analyzed in, a certificate less cryptography may subject to two types of adversary: Type *I* adversary may request entity's public keys and replace public keys with values of its choice but is not allowed to access the master private key; and Type *II* adversary may access to the master private key but is not allowed to replace the public keys of the entities. The security of a CLGSC scheme includes confidentiality for the signcryption and encryption modes, and enforceability for the signcryption and signature modes. The security proof of a CLGSC scheme can be viewed as an interactive game between a challenger *C* and an adversary *A*. There are four games for confidentiality and enforceability proof between the challenger, and Type *I* adversary and Type *II* adversary, respectively gives detailed descriptions for the four games. To avoid reinventing the wheel, we refer to [16] for the security model for a CLGSC. We directly give the definitions based on the games.

IV. ALGORITH

Advanced Encryption Standard:

AES is based on a design principle known as a substitution-permutation network, a combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a particular finite field.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input,

called the plaintext, into the final output, called the cipher text. The number of cycles of repetition are as follows:

a) 10 cycles of repetition for 128-bit keys.

b) 12 cycles of repetition for 192-bit keys.

c) 14 cycles of repetition for 256-bit keys.

AES is based on a design principle known as a substitution-permutation network, a combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4 × 4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a particular finite field.

$x^8+x^4+x^3+x+1.$

VI. RESULT ANALYSIS

In the wake of executing some piece of framework we got framework execution on agreeable level. The beneath table demonstrates the principal calculation execution for client plain information change too encryption unscrambling.

TABLE I.TABLE OF SYSTEM PERFORMANCE

Data size in MB(Megabyte)	Encryption Time (Milliseconds)		Decryption Time (Milliseconds)	
	Existing	Proposed	Existing	Proposed
5	595	505	724	599
10	1120	1016	1132	1021
15	1680	1534	1687	1538
20	2260	2054	2231	2021

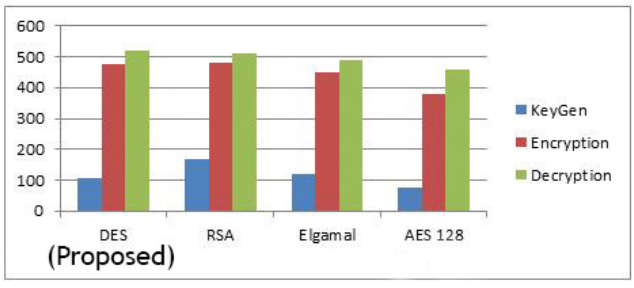

Fig. System Result Graph

Here above graph shows the system performance for cryptography algorithm. X shows the plain data size and Y show times required in Milliseconds. The base on analysis it is more efficient than all existing cryptographic techniques

CONCLUSION

Here we are implemented the new technology based on android system. Here, the patient status is automatically transferred to the mobile application. We implement attribute based Encryption technique for data security , Attribute based Encryption means Key generator generate encryption key based on Requested Authority Example Doctor, Nurse, Relative .can view full patient information if Request Authority is Doctor . Others cannot view full patient information. But some cases, the data produced may be requested by authorized person like doctor, he can monitor and he can able to suggest the prescription or medicine to the patient. But others, like nurse or a relatives requested for monitoring, we eliminate the trust we put on the data sink by encrypting the stored data at the data sink. Thus the data sink itself has no access to the original data, so they can only view the data's.

FUTURE WORK

The current architecture is very efficient for security purpose, but sometime it's utilized multiple resources. When such a system allocates multiple resources it will generate a lot of dependencies. For the next updation we can focus on minimum resources utilized with system flexibility like power vm, network, memory, etc.

REFERENCES

[1] C. Lin, P. Wang, H. Song, Y. Zhou, Q. Liu, G. Wu, "A differential privacy protection scheme for sensitive
Big data in body sensor networks," *Annals of Telecommunications*, 2016, ISSN 0003-4347.

[2] A. Siva Sangari, J. Martin Leo Manickam, "Secure Communication over BSN Using Modified Feather
Light Weight Block (MFLB) Cipher Encryption," *Journal of Software*, vol. 10, pp. 961, 2015, ISSN
1796217X.

[3] T. Hayajneh, B. Mohd, M. Imran, G. Almashaqbeh, A. Vasilakos. "Secure Authentication for Remote
Patient Monitoring with Wireless Medical Sensor Networks," *Sensors*, vol. 16, pp. 424, 2016, ISSN 1424-
8220.

[4] Y. Zhou, B. Yang, W. Zhang, "Provably secure and efficient leakage-resilient certificate less signcryption

Scheme without bilinear pairing," *Discrete Applied Mathematics*, vol. 204, no. 5, pp. 185202, 2016.

[5] M. Chase and S. Chow, Improving privacy and security in multi authority attribute-based encryption, in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp.

121130.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing, in INFOCOM10. IEEE, 2010, pp. 534542.

[7] K. Yang, X. Jia, and K. Ren, Attribute-based fine-grained access control with efficient revocation in cloud storage systems, in AsiaCCS13.ACM,

2013, pp. 523528.

[8] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems, IEEE Trans. Info. Forensics Security, vol. 8, no. 11, pp. 17901801, 2013.

[9] Wei Li, KaipingXue, YingjieXue, and Jianan Hong, TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage, IEEE Transactions on Parallel and Distributed Systems,Vol. PP,Issue 99, pp.1- 12, 2015.

[10] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE, Privacy Preserving Delegated Access Control in Public Clouds, IEEE Transactions on Knowledge and Data Engineering, Vol. 26, Issue 9, pp.2268-2280, 2014.

[11] Kan Yang, Student Member, IEEE, and XiaohuaJia, Fellow, IEEE, Expressive, Efficient, and Revocable Data Access Control for MultiAuthority Cloud Storage, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue 7, pp. 1735-1744,2014.

[12] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and MircoMarchetti, Scalable Architecture for Multi-User Encrypted SQL Operations on Cloud Database services", IEEE Transactions on Cloud Computing, Vol.

2, Issue4, pp. 448-458, 2014.

[13] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and MircoMarchetti, Performance and cost evaluation of an adaptive encryption architecture for cloud databases, IEEE Transactions on Cloud Computing, Vol. 2, Issue 2,pp.143- 155, 2014.

[14] Luca Ferretti, Michele Colajanni, and MircoMarchetti, Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue 2, pp.437-446,2014