International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Certificate Less Generalized Signcryption (CLGSC) D2D-assist Data Transmission Protocol for Mobile Health-Systems

J. Jessi Kohila[1], B. Shanmuga Sundari M.E[2], A. Mymoon Abdul Basiriya M.E[3]

[1]*PG Scholar, Department of Computer Science & Engineering, PET Engineering College*
[2,3] *Professor, Department of Computer Science & Engineering, PET Engineering College*

ABSTRACT- *The rapid advancement of technology, healthcare systems have been quickly transformed into a pervasive environment, where both challenges and opportunities abound. On the one hand, the proliferation of smart phones and advances in medical sensors and devices have driven the emergence of wireless body area networks (WBAN) for remote patient monitoring, also known as Mobile-Health (M-Health), thereby providing a reliable and cost effective way to improving efficiency and quality of health care. On the other hand, the advances of M-Health systems also generate extensive medical data, which could crowd today's cellular networks. Device-to-Device (D2D) communications have been proposed to address this challenge, but unfortunately, security threats are also emerging because of the open nature of D2D communications between medical sensors and highly privacy-sensitive nature of medical data. Even more disconcerting is healthcare systems have many characteristics that make them more vulnerable to privacy attacks than in other applications. To propose a Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol for M-Health systems by using Certificate less generalized Signcryption technique.*

Keywords: D2D Communications; Mobile-Health Systems; Security; Certificate less sign cryption; Key generation center.

I. INTRODUCTION

Mobile-Health (M-Health) system has been envisioned as a promising approach to improving healthcare quality and save lives in the aging society . In M-Health systems, the Personal Health Information (PHI) is collected by Body Area Network (BAN) and aggregated by smartphone. 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. 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 the ID-based public key cryptography is solved. Additionally, the CLPKC avoids the problem of certificate revocation, storage and distribution in certificate-based public key cryptography.

II. PROPOSED SYSTEM

The 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 the ID-based public key cryptography is solved. Additionally, the 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.

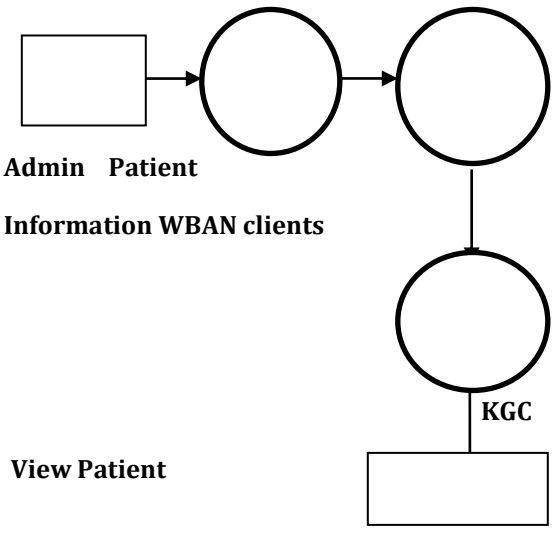

Fig2.1 Architecture Diagram

A) Wireless Body Area Network Clients (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. A body area network (BAN), also referred to as a Wireless Body Area Network (WBAN) or a body sensor network (BSN), is a wireless network of wearable computing devices. BAN devices may be embedded inside the body, implants, may be surface-mounted on the body in a fixed position Wearable technology or may be accompanied devices which humans can carry in different positions, in clothes pockets, by hand or in various bags.

B) Network Manager: 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.

C) Key Generation Center (KGC): Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. A device or program used to generate keys is called a key generator or key gen.

D) Medical Service Provider: 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.

III. RESULTS AND DISCUSSION

A) The Proposed CLGSC Algorithm:

The proposed CLGSC scheme is composed by the following four algorithms: Setup(k). Given the security parameter k, the KGC generates two primes p and q such that q|p − 1. P is a generator of cycle group G, which is on ECC with order q. the KGC randomly selects $xN \in Z * q$ as the master private key and computes the public key XN = xN P. Moreover, the KGC chooses three secure hash functions:

- $H1 : \{0, 1\} * \times G \times G \times G \rightarrow Z * q$,
- $H2 : Z * q \times Z * q \rightarrow Z * q$,
- $H3 : Z * q \times Z * q \rightarrow \{0, 1\} *$.

Define an index function f(ID) as follows:

f(ID) = 0 if ID = ø,
otherwise f(ID) = 1.

The system parameter is published as params = (p, q, P, XN , H1, H2, H3). KeyGeneration(IDi).

The algorithm is performed by the user IDi and the KGC interactively. The user IDi randomly selects $xi \in Z * q$ as the secret value and computes Xi = xiP as its partial public key. The user sends its identity and partial public key (IDi , Xi) to the KGC. The KGC randomly selects $yi \in Z * q$ and computes

Yi = yiP,
zi = yi + xN H1(IDi , Yi , Xi , XN)

for the user with partial public key Xi .The partial private key zi is sent to the user through secure channel and the public key (Xi , Yi) is stored in the public tree by the KGC. The full private key of user IDi is (xi , zi). The full public key is (Xi , Yi). Note that IDi may judge the validity of the partial private key by checking whether Yi + H1(IDi ,Yi, X ,XN)XN = ziP. CLGSC(IDA, IDB, m). With IDB as the receiver, Signcryption (signature or encryption) of the message m is performed by the sender IDA as follows:

- Computes f(IDA), f(IDB); IDA randomly picks $r \in Z * q$,
- and computes h1 = H1(IDB, YB, XB, XN);
- Computes f1 = rP, f2 = rf(IDA)/(xA + zA + f3), f3 = H2(f1, IDA, m);
- Computes $m' = (H3(v1, v2)f(IDB)) \oplus m$,

where v1 = rXB, v2 = r(YB + h1XN);
Return μ = (f1, f2, f3, m′) as the ciphertext. UCLGSC(IDA, IDB, μ)..

- Computes f(IDA), f(IDB), h ′ 1 = H1(IDA, YA, XA, XN);
- Computes v ′ 1 = xBf1, v ′ 2 = zBf1, m = (H3(v ′ 1 , v′ 2)f(IDB)) ⊕ m′ ;
- Checks H2(f2(XA+YA+h ′ 1XN +f3P), IDA, m) = f3

If the equation holds, the message is accepted.

- Correctness of the encryption: m = H3(v ′ 1 , v′ 2) ⊕ m′ = H3(xBf1, zBf1) ⊕ m′ = H3(rXB, r(yB + xN H1(IDi , Yi , Xi , XN)P)) ⊕ m′ = H3(v1, v2) ⊕ m′ = m

- Correctness of the signature: H2(f2(XA + YA + h ′ 1XN + f3P), IDA, m) = H2(r xA + zA + f3 (xAP + zAP + f3P), IDA, m) = f3. B. Security proof In this subsection, we give the security proof of the proposed CLGSC scheme in the random oracle model.

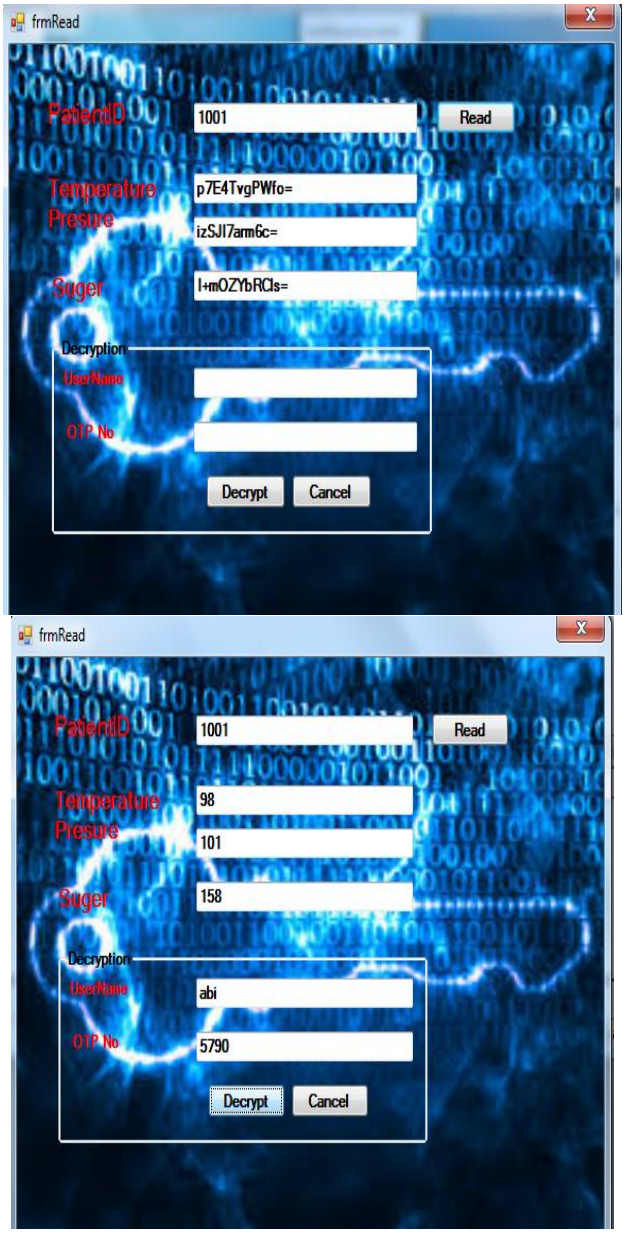

Fig: 3.1 Patient Records Encrypted Decrypted Image

IV. CONCLUSION

To proposed a new efficient certificate less generalized signcryption (CLGSC) scheme, which is proven to be secure in confidentiality and enforceability in the ROM under the DLP and CDHP assumption. Based on the proposed CLGSC scheme, we designed a lightweight and robust security-aware (LRSA) D2D-assist data transmission protocol for M-Health systems. Security analysis demonstrated that the LRSA protocol can achieve data confidentiality and integrity, mutual authentication, contextual privacy, anonymity, unlink ability, as well as forward security. Moreover, the LRSA protocol outperforms the existing schemes in terms of computational and communication overhead. For future work, we will consider relay selection strategies for the security-aware D2D-assist data transmission for M-Health systems.

REFERENCES

[1] Ahmed. M, Ahamad. M ,and Jaiswal.T Augmenting security and accountability within the e Health Exchange," IBM Journal of Research and Development, vol. 58, no. 1, 8:1-8:11, 2014.

[2] Al-Riyami.S , and Paterson.K,"Certificate less public key cryptography," Advances in Cryptology-Asiacrypt2003, Lecture Notes in Computer Science, Springer-Verlag 2894: 452-473, 2003.

[3] Barua.M, R. Lu, and X. Shen, "SPS: Secure personal health information sharing with patient-centric access control in cloud computing," IEEE Global Communications Conference, pp. 647-652, 2013

[4] Bellare.M, and Rogaway.P, "Random Oracles are Practical: a Paradigm for Designing Efficient Protocols," ACM CCCS, pp. 62-73, 1993.

[5] David.P, and Jacque.S, "Security arguments for digital signatures and blind signatures," Journal of Cryptology, vol. 13, no. 2, pp. 361-396, 2000.

[6] Diffie.W, and M. E, "Hellman New directions in cryptography," IEEE Transactions on Information Theory, IT-22: 644-654, 1976..

[7] Fragopoulos. A.G, J. Gialelis1, and D. Serpanosl, "Imposing Holistic Privacy and Data Security on Person Centric e Health Monitoring Infrastructures," 12th IEEE International Conference on e-Health Networking Applications and Services (Health com), 2010.

[8] Guo.L, C. Zhang, J. Sun, Member, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," IEEE Transactions on Mobile Computing, vol. 13, no. 9, pp. 1927-1941, 2014.

[9] Ji.H.F, W. B. Han, and L. Zhao, "Certificate less generalized sign cryption,"Cryptology e Print Archive, Report 2010/204.

[10] Kushwah.P, and S. Lai, "Efficient generalized signcryption schemes," Cryptology e Print Archive, Report 2010/346.http://eprint.iacr.org(2010)