Internet of Things (IoT) based cloud security for health care

N.Aishvarya Sree[1], S.Jasmine Monisha[2], Mrs.R.Kalpana[3], Dr. P.Veeralakshmi[4]
[1],[2]– Students, Department of IT, Prince Shri Venkateshwara Padmavathy Engineering College.
[3] – Assistant Professor, Department of IT, Prince Shri Venkateshwara Padmavathy Engineering College.
[4] – Associate Professor, Department of IT, Prince Shri Venkateshwara Padmavathy Engineering College.

Abstract— Enhancement of a promising and efficient key distribution is the cornerstone of security for which cryptog-raphic methods are applied to guard the privacy of smart devices in the internet of things (IoT). However, when using conventional key distribution in real time mobile services, it is usually deficient to build multiple channels with strong security simultaneously on a single data server. Therefore, we focus on preserving privacy of client records in health care applications by collecting or monitoring real time and remote data com-monly observed using Identity – Based Key Encapsulation Mechanism. Further, we operate the one-pass communication with asymmetric key distribution which avoids data leakage. Using data table that is created inside the cloud for storage, the data dropout is rectified. Our instantiated system provides strong security on real time services over cloud IoT..

Keywords- IoT, asymmetric key distribution, Identity-based key encapsulation mechanism, one-pass communication, Provable security.

I. INTRODUCTION

Mobile services, with the development of smart devices like emerging wearable sensors, are important building blocks for the Internet of Things (IoT). Those smart devices are the potential sources that senses large amounts of data at the periphery of the IoT, and also possess mobility along with people or vehicles and sufficient computational capability for complex operations. These services bring many conveniences for avoiding security risks while mobile clients apply smart devices to register the services. Since their personal privacies (especially identities) are bound to the smart devices, Mobile services rely on wireless media for communication, and personal data can be easily leaked to outsiders. Consequently encrypting outsourced data using cryptographic methods, it is a promising approach to preserve the confidentiality of the data with provable security during transmissions. However, before ensuring the confidentiality of the data, the preliminary

task for establishing secure mobile services is key distribution. Key distribution is important for establishing secure services. In previous work, it has been shown that smart devices establishing secure networking using Symmetric keys with computationally robust nodes has strong security than trust-relied systems. Though several works have been proposed for wireless channel secret key extraction techniques that can avoid communications for distributing keys, key distribution techniques are still indispensable to the security of the IoT in many cases. Especially, wireless channel key extraction techniques are not applicable through long-distance communication between a server and its clients. For example, key extraction techniques are unavailable in a common scenario of the IoT for health care where the server is a doctor in a hospital, and the clients are patients at home. But, it is impossible to compute a pair of encryption and decryption keys from different wireless channels. And wireless channel secret key extraction techniques hardly provide provable security, which has been a popular requirement for a secure key distribution. The necessity of asymmetric key distribution approach for mobile real-time services in the IoT is the inspiration of our work. Especially, the monitored medical data for health care are highly related to personal privacy, which should be normally transmitted as cipher texts. Only the specially authorized data managers can read the real data. Such scenarios, occurring to support a doctor monitoring patients' health condition in long distance, has requirements on real-time and high efficiency with multiple individual session keys for multiple mobile clients. To achieve our goals, we face the main challenge of data dropout that is avoided with the creation of data table in the cloud. The data table resolves the problem of offline data loss and dropout from the client. Although non-interaction key distribution [12] has a trivial cost for key distribution, it cannot guarantee ultimate security for the multiple clients in a single server. Conseq-uently, if a key distribution protocol with only one-pass communication for multiple mobile clients in batch can be realized in a mobile service system, the system will sharply enhance the communication efficiency while keeping all security satisfactions.

II. RELATTED WORK

Several works prefer cryptographic methods because of the provable security they applied. In this section we review the previous works and some correlated researches on secure and efficient mobile services. Conditional identity based broadcast proxy re-encryption [17] is used on recognizing the expected collector, intermediary appoints the re-encoded key to the beneficiary utilizing the information to be decoded. However, block level operations on encrypted data blocks the insertion, deletion and update operations which needs to be considered to reduce the burden of data owner and secure the services. By introducing cryptography to WSN, establishing a secure network through pre-distributed keys or keying materials to encrypt plaintexts and then exchanging cipher texts by computationally robust nodes, applying cryptography show much stronger security than trust-relied system [10]. Wang [1] proposed a key distribution protocol slightly similar to our work, which is evoked by mobile clients while preserving the mobile client's anonymity. Although, it still focuses on the key distribution for end-to-end communications. It fails on key distribution in batch for multiple mobile clients. And their key distribution protocol hardly works while being combined with the cloud. Specially, the protocol is unable to guarantee the anonymity of clients when delegating their key distribution works to the cloud.

Key Distribution Protocols: Key distribution protocol is essential to realize our secure and practical real-time mobile services. We compare three categories of key distribution protocols which are commonly used in previous work: non-interactive key distribution, key agreement, and one-pass key distribution. Both in the non-interactive and one-pass key distribution protocols, clients need to register and obtain their private keys before distributing session keys. This new model allows multiple data managers to confidentially distribute different session keys to their intended mobile clients online or offline with the assistance of the cloud, and improve the security requirements according to the new model. The original model allows one data manager to distribute his session keys. In addition, the original instance of our services requires a data manager directly broadcasting IBKEM encapsulation to the intended mobile clients. Hence, the original instance is suitable only for the scenario where all mobile clients remain online. In contrast, the new instance in this paper achieves search over IBKEM encapsulations and allows multiple data managers to distribute their session keys with the assistance of the cloud at both online or offline.

III. SYSTEM DESIGN

In the existing system, wireless channel secret key extraction technique is used.The received shared key will be used by both the sender and receiver for encryption anddecryption of messages.Only remote area can process the system for communication between doctor and patient while online.Wireless channel key extraction technique is not applicable through long distance communication.It is difficult to compute pair of encryption and decryption keys from different wireless channels.Data leakage is possible since same key is used for both sides.Data dropout rate is high during unnoticed off-hours.

Key distribution phase: The Trusted-Third Party generates private keys using symmetric encryption protocol for both registered doctors and patients. Therefore the key generated can be easily leaked to the unauthorized third parties with minimum effort as shown in fig 1.1.

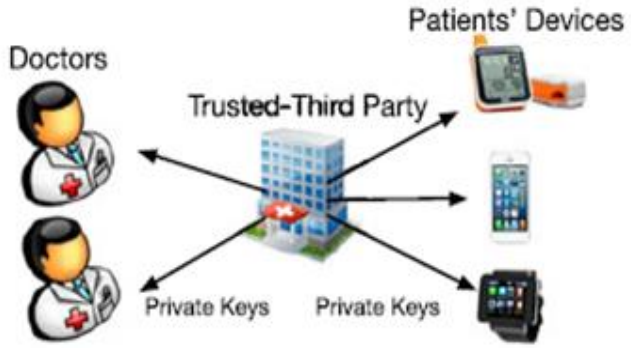

Fig 1.1. Key distribution phase

In the proposed system, we instantiate a secure and practical real-time mobile services by applying the introduced IBKEM scheme. As results, two instances are provided. The one is online transformation via cloud, the other is offline transformation. Offline transformation is termed with a data table inside the cloud server. The proposed design overcomes the difficulties of wireless channel key extraction techniques, Identity-Based Key Encryption Mechanism (IBKEM) is formulated for strong security and efficiency. It initiates provable security with asymmetric key function for specially authorized server and client. IoT cloud is driven with Raspberry Pi sensor kit to enhance the mobile clients records. Security requirements such as data leakage, data dropout is reduced with high personal privacy. Different wireless channels and long distance communication between the doctor and patient is enabled. Data table is created at the cloud to store all the updations even when the doctor is offline. The main inspiration work is the novel key distribution approach in the mobile real-time services in the IoT.

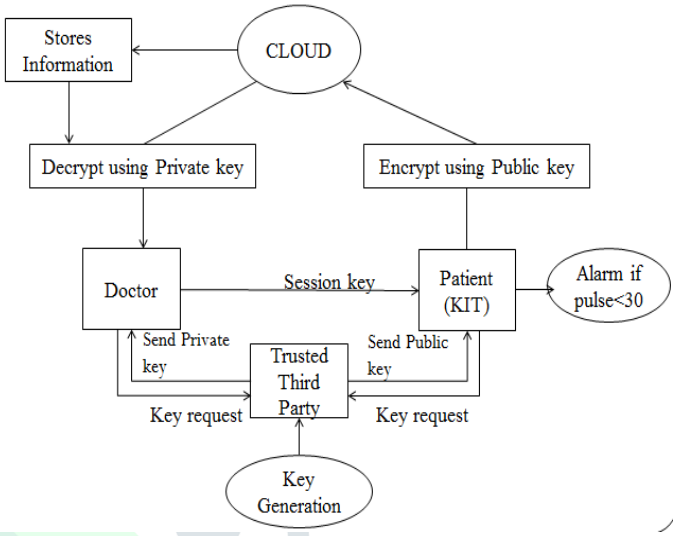

Fig. 1.2 block diagram

Fig 1.2 represents the process and the workflow of the system enhanced with the IoT kit. It is the overall communication of the doctor and the client.

List of Modules:

1. **Registration and Key Distribution:**

The Trusted Third Party (TTP) is the system organizer of the real-time mobile services. It initializes the system parameters and generates private and public keys for all registered data managers and mobile clients. The system registers the doctor and patient details in hospital website. The TTP selects a doctor based on patient's disease. The TTP generates a private key and public key for each doctor and patient respectively.

2. **Session Key Generation**

The Doctor(data manager) can generate session key for each kit(mobile client). Session keys are used periodically to encrypt the personal records of the mobile clients, and the resulting cipher texts can be decrypted by the intended data managers.RSA algorithm is used here to provide asymmetric key for encryption and decryption technique. Data managers organize real-time mobile services. First they distribute session keys to the corresponding mobile clients online or offline with the assistance of the cloud for the security of these clients and their uploaded data.

3. Decrypt the cloud data:

The encrypted cloud data will be sent to the doctor to get the original information.The data decryption process is carried in two phases:i) online transformation, ii) offline transformation. When doctor is online, The data manager can control the data as usual through the cloud. The sensed values is decrypted using the corresponding private key.Session cookies are read by the cloud to know if the doctor is online or offline.When the doctor is offline, the sensed values are all sent to the **data table** inside the cloud.This data table is used to store the encrypted data using IBKEM mechanism.The encrypted data that is stored in the sql data table will be flushed out to the doctor portal once his session turns online.

IV. MATHEMATICAL MODEL

The RSA protocol implementation

Let S be the Whole system S= {I, P, O}
I-input
P-procedure
O-output
Input I-
M = { Hi }
Where,
M- message
Procedure(P)-
{message, prime factorization, cipher text(encryption), plain text(decryption) }
Step1: Message
In this step primarily user provides message. So input is plain text file, which is selected for convertion of cipher text. The file is converted to encrypted format and uploaded on cloud.
Plain text M= "hi"
Step2: Encryption
M=''hi"->89 which is the key(trapdoor) for M
Let us consider two prime numbers for factorization of M
P1=53
P2=59
Prime factorization N is calculated for public key
N=p1*p2=3127
Φ(N) = (P1-1)(P2-1)=3016
Here, Φ(N)_ defines the measure of breakability of a number.
The encryption (cipher text), C= M^e mod N
⇨ $(89)^3$ mod 3127 = 1394
Therefore, C=1394
Step 3 Decryption
The private key generated using d
d= [2*(Φ(n)) + 1]/ e
⇨ [2*(3016) + 1]/ 3
⇨ d= 2011
Using private key let decryption is formulated as,
$(C)^d$ mod N= M

$(1394)^{2011}$ mod 3127 = 89 "HI"
M={"HI"} is found as result.

Output(O)-
To decrypt the message, C is given to the data manager and the value of N, C, E is given to the cloud for access of public key.

S= { I ; P(message, prime factorization, cipher text (encryption), plain text(decryption)) ; O }
S= {"HI" ; (M=89, N=3127, C=1394 ,M=89) ; "HI" }

V. RSA ENCRYPTION AND DECRYPTION

Data cannot be easily decrypted using the known public key. Strong Security on both encryption and decryption side. The main challenge of Data leakage is overcome with RSA algorithm. Highly secured with different keys to be broken. easier to implement than elliptical curve. Data leakage is avoided with private key at decryption. Data dropout is overcome with the concept of data table for offline storage. Anonymous access is not possible in RSA implementation. Different wireless channels can have better efficiency in access to the proposed system.

Identity Based Key Encapsulation Mechanism (IBKEM) scheme:
With this scheme, one data manager is able to distribute multiple individual session keys to multiple mobile clients in batch with limited expenses. These mobile clients can confidentially upload their real-time personal records for online data retrieval. The system is suitable for clients having unstable network channels also. Therefore the proposed scheme is essentially provable for security and high efficiency as demonstrated by analyses.

VI. KIT CONFIGURATION

In the proposed system model we use Raspberry Pi sensor kit. The pulse sensor kit connected to the patient to fetch the value and encrypts using session key and doctor's public key and send to the doctor. When doctor is online the kit data will be directly displayed in doctor's webpage via cloud application. Thus Cloud plays the assisting role by storing data when doctor is offline i.e. Incase doctor status is offline the data will be stored in the cloud. When the doctor gets online the data will be flushed to doctor application.

The Raspberry Pi kit focuses of two sensors,

i) Room temperature and heart beat sense-
- The kit starts sensing the process once the session key is generated by the data manager.
- The heart beat sensor senses the rate of every minute on turns.
- The room temperature is noted at the same rate.
- The values are passed in cipher texts to avoid data leakage.

ii) Buzzer for emergency.-
- Buzzer ring is continuous and can be stopped only by the doctor.
- The emergency alarm is also given to the doctor as a record of patient.
- The buzzer rings as an alarm when the pulse rate goes below 30.

VII. SECURITY REQUIREMENTS

Key distribution phase: Public key is distributed to the registered mobile client for encryption of data.Private key is distributed to the corresponding data manager for the data decryption.The keys are generated using asynchronous key generation function.

Data retrieval phase: Session key is generated to the client once the data manager logs in.RSA algorithm provides asymmetric keys to provide strong security against attackers. Once session key is given, the kit starts sending its sensing values to the cloud. The cloud contains data table in encrypted format of cipher texts. IBKEM is used to encapsulate the sensing values in the sql data table inside the cloud storage. Personal privacy is maintained by using cipher text encryption on the client side.

VIII. CONCLUSION

A systemfor real time mobile services is established with data confidentiality and the anonymity of records.With this proposed system, data manager can retrieve personal records of clients online or offline with the cloud assisted IoT. This system is proposed mainly for healthcare services and traffic management with satisfied security models using IBKEM scheme. When the proposed RSA protocol is formulated with larger keys to resolve, it takes years even by the most powerful network of computers to breakthrough the trapdoor. The trapdoor is a one way function that is easy to compute in one direction while is absolutely hardest to reverse the process unless the manager has any special information.

XI. REFERENCES

[1] W. Wang, P. Xu, and L.T.Yang, "One-pass anonymous key distribution in batch for secure real-time mobile services," in Proc. IEEE Int. Conf. Mobile Services, 2015, pp. 158–165.

[2] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Commun. Mag., vol. 48, no. 9, pp. 140–150, Sep. 2010.

[3] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Netw., vol. 32, pp. 17–31, 2015.

[4] C.Doukas, I.Maglogiannis, V.Koufi, F.Malamateniou, and G. Vassila copoulos, "Enabling data protection through PKI encryption in IoT M-health devices," in Proc. IEEE 12th Int. Conf. Bioinf. Bioengineering, 2012, pp. 25–29.

[5] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the Internet of Things," Comput. Elect.Eng., vol. 37, no. 2, pp. 147–159, 2011.

[6] D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, "Secure data processing framework for mobile cloud computing," in Proc. IEEE Conf. Comput. Commun. Workshops, 2011, pp. 614–618.

[7] R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, "The potential of Internet of M-health Things m-IoT for non-invasive glucose level sensing," in Proc. Annu. Int. Conf. IEEE Eng. Med.Biol. Soc., 2011, pp. 5264–5266.

[8] Y. Wang, D. S. Wong, and L. Huang, "One-pass key establishment model and protocols for wireless roaming with user anonymity," Int. J. Netw. Secur., vol. 16, no. 2, pp. 129–142, 2014.

[9] L.B. Oliveira, et al., "Tiny PBC: Pairings for authenticated identity based non-interactive key distribution in sensor networks," Comput. Commun., vol. 34, no. 3, pp. 485–493, 2011.

[10] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target driven applications," Comput. Secur., vol. 37, no. 9, pp. 111–123, 2013.

[11] M. Abdalla, D. Catalano, and D. Fiore, "Verifiable random functions: Relations to identity-based key encapsulation and new constructions," Cryptology, vol. 27, no. 3, pp. 544–593, 2013.

[12] C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare,"
in Proc. 6th Int. Conf. Innovative Mobile Internet Services Ubiquitous Comput., 2012, pp. 922–926.

[13] M. B. Paterson and D. R. Stinson, "A unified approach to combinatorial key predistribution schemes for sensor networks," Des. Codes Cryptography, vol. 71, no. 3, pp. 433–457, 2014.

[14] S.Ruj, A.Nayak, and I. Stojmenovic, "Pairwise and triple key distribution in wireless sensor networks with applications," IEEE Trans. Comput., vol. 62, no. 11, pp. 2224–2237, Nov. 2013.

[15] L. Zhang, "Provably secure certificate less one-way and two-party authenticated key agreement protocol," in Information Security and Cryptology, T. Kwon, M.-K. Lee, and D. Kwon, Eds. Berlin,
Germany: Springer, 2013, pp. 217–230.

[16] E. Okamoto, "Key distribution systems based on identification information," in Advances in Cryptology. Berlin, Germany: Springer, 1988, pp. 194–202.

[17] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity based broadcast proxy re-encryption and its application to cloud email," IEEE Trans. Comput., vol.65,
no. 1, pp. 66–79, Jan. 2016.

[18] J. Davies, Implementing SSL/TLSUsing Cryptography and PKI. Hoboken, NJ, USA: Wiley, 2011. 862 IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL.11,NO.september/October 2018 .

[19] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Trans. Comput., vol. 62, no. 11,pp. 2266–2277, Nov. 2013.