Secure key encapsulation and distribution mechanism for real time secure mobile services

Sunayana S. Bisalapur[1], Mr. Rohit B. Kaliwal[2]

[1] PG Student, Department of Computer Network Engineering, Visvesvaraya Technological University, Belagavi
[2] Assistant Professor, Department of Computer Network Engineering, Visvesvaraya Technological University, Belagavi

---***---

Abstract - *The vast demand of cloud for storage purpose in every organization has led to many challenges in terms of security and privacy. There is new challenge in providing security to the data stored in cloud. Security has emerged many new techniques one of the technique is the Identity Based Key Encapsulation Mechanism which is a unique mechanism of securing the data exchange. The novel scheme used has capability of keeping the data more confidential and for better performance results this new scheme is compared with another scheme called Quantum Key Distribution technique. The result is examined for both of them showing IBKEM has good performance than the QKD.*

Key Words: Cryptography, Identity Based Key Encapsulation mechanism, Cipher-text policy Attributed based encryption, Quantum Key Distribution.

1. INTRODUCTION

The data transfer in the wireless communication has many of the ups and downs it may lead to the wrong communication or miss communication or else some attacker may find the valuable data while the data is sent from one place to another. Security to the data must be provided when used for communication. In the internet world also there are many of disadvantages leading to spoil the whole system. Care has to be taken a lot, in the business environment some confidential information will be stored and some may take the advantage of leaking the information. In such cases the data has to be stored and it should have passwords to keep it secret or else there has to be one admin authority to look after these all. The main security term best suites when the data is to be transferred to another place this is more challenging that the data has to be sent as it is without any changes to the data.

Key distribution has been emerged attaching key to data while sending it and disclosing the data when it is received at the other place. Several techniques has been introduced, one of the techniques which is the new scheme has the unique method of distributing the key for the exchange of the data is the Identity Based Key Encapsulation Mechanism which has a kind of uniqueness in protecting the data. Along with this another scheme is just used for analysis comparison is the quantum Key Distribution which is also a key distribution technique which has different method of protecting the data by using the sequence of q bits involving quantum mechanics in it making data very confusing when the eves dropper tries to hack the key. Thus the two methods are involved where the IBKEM is concentrated as main part of this for the implantation and the other is just used for the comparison to know whether the present is better or not. Then for storing the data the cloud platform is used. The data is also encrypted using the attribute based encryption and the encrypted data is saved in the cloud to avoid the misplacing or possibility if exchanging wrong data. Thus the data is encrypted in the cloud even if the eavesdropper tries to change the data it must be more difficult for attacker too. The data will be decrypted only to those users who have the actual key with them.

2. LITERATURE SURVEY

The data security and privacy in remote health care monitoring system with the security authentication protocols is proposed [1]. The algorithm for authentication is used is Rabin algorithm for authentication commands in a secured manner. The digital signature is added to the algorithm. The result is verified by using MIRACL software which shows that rabin algorithm is much more secure than other cryptographic algorithms.

A new quantum key distribution that generate secret key using the photons and to simulate the same using C programming language is done [2]. There are two parts first part includes the introduction of QKD protocol and the final one includes the BB84 protocol with two steps involved. The simulation of BB84 protocol is done. During the simulation particular threshold for data loss was chosen to decide the presence of intruder and in such case whole sequence of bits are discarded and retransmission is requested.

The main goal of this paper involves key distribution in IOT scenario considering security for mobile services [3]. The high level security and efficiency is to be achieved. The main goal involves key distribution in IOT scenario considering security for mobile services. The high level security and efficiency is to be achieved. The result achieves confidentiality and anonymity of data retrieval from the multiple clients.

The relation between verifiable random functions and the IBKEM is proposed [3] such that it is VRF suitable that should produce unique decapsulation mechanism. It should satisfy unique decapsulation and pseudo-random decapsulation and a new VRF suitable IB-KEM based on the Bilinear Diffie–Hellman Inversion assumption is proposed. In this a new methodology is introduced to construct verifiable random functions from a class of identity-based key encapsulation schemes that is called VRF-suitable and the applicability of methods by providing two concrete realizations of the new primitive is shown.

The survey is done on new trend of cryptography called bilinear mapping [5]. Elliptic curve cryptography is considered for mapping as it has several advantages. To conclude this gives overview of the bilinear mapping how they are used to design identity based encryption signature that are provably secure.

The authentication mechanism is proposed [6] in the cloud infrastructure lacking in the security. The method involves using quantum key distribution mechanism that resolves the problem of unauthorized access to the network. The survey is done on security why it is needed and secondly the quantum theory is considered to perform safe communication between two parties. In the future work reduced key size is considered for better security with involvement of quantum key distribution.

3. EXISTING SYSTEM AND PROPOSED SYSTEM

A. Existing System

In the existing system the main concentration is on the analytical explanation of the novel scheme used. The compilation platform is not the web based one and as the data are uploaded in the cloud there is no encryption technique involved, rather the key is distributed by the third party then data will be uploaded in the cloud as it is. So the encryption is needed in the cloud for more security.

B. Proposed System

In the proposed system the actual working of the Identity Based Key Encapsulation Mechanism is examined about how the cloud account is linked and data uploaded and downloaded from the cloud is also seen. The IBKEM scheme involves four algorithm for distributing the key as well as encryption of the data. The proposed model is shown in the Fig.1 where there is a scenario of doctor monitoring the patient through cloud. In this firstly

1. Admin will be looking after all the data and the registration process is involved for giving ID to each and every user who does the registration.

2. After the registration the patient who enters the hospital will be registering in the hospital and they will be given Id and then doctor will be allotted to patient by the admin.

3. After the allotment the doctor will monitor patient record in batch by running particular Id of the patient.

4. The record will be uploaded to the cloud in the encrypted format as the Cipher text policy is used while the monitoring is done.

When doctor itself wanted to see the record he will just have to login and select the patient Id, he/she will get the record detail in the decrypted format i.e. only the doctor will be getting the actual record of the patient. Thus the secured data is going to be transferred as there will be no mixing up of the patient records when there are n numbers of patients.

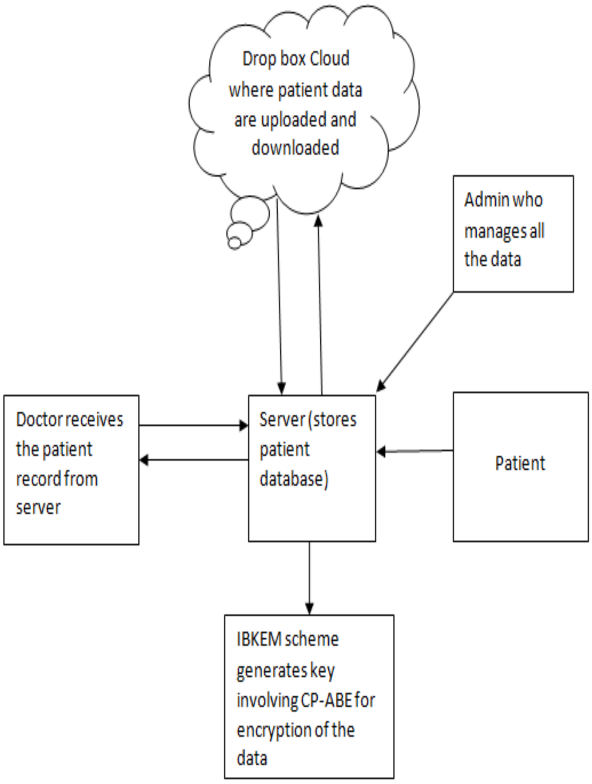

Drop box Cloud where patient data are uploaded and downloaded
Admin who manages all the data
Doctor receives the patient record from server
Server (stores patient database)
Patient
IBKEM scheme generates key involving CP-ABE for encryption of the data

Fig -1: Proposed architecture of the system

4. IMPLEMENTATION

The architecture of the system consists of the following:

1. Admin
   Admin whose main task is to look after all the data stored in the cloud as well as the monitoring task.
2. Doctor
   After the registration the doctor will be an authorized user who is going to monitor the patient in batch.
3. Patient
   The patients will be given their own identity when registering in particular hospital.
4. Server
   It is the one which maintains the whole record of the patient and it is one where the monitoring task is done.

5. Cloud
   The cloud platform is used for the storage of personal record of each and every patient.

Identity based Key Encapsulation Mechanism consist of four algorithms:

1. Setup phase:
   In this phase, the trusted third party chooses security parameter which generates key.
2. Extraction phase:
   In this phase private key is generated.
3. Encryption:
   This method is used to encrypt the file by using the public key known.
4. Decryption:
   Encrypted file will be decrypted by the private key.

In Quantum key distribution the example is taken where person A and person B are considered and the program is run as client and server to check where they both are communicating or not.

5. RESULT

In the result analysis as said using the IBKEM the algorithms are run to generate the key as well as encrypt the data. The encrypted data is stored in the cloud as shown in the Fig.2.

When the registered doctor will login and access the patient details the details of the patient will be available in the decrypted format to the authorized doctor as shown in Fig.3.the actual health rate is available. Thus storing the data more secure and making that data available only to authorized user.

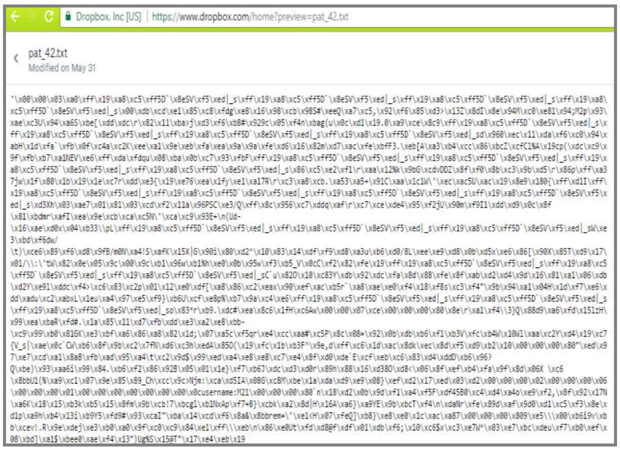
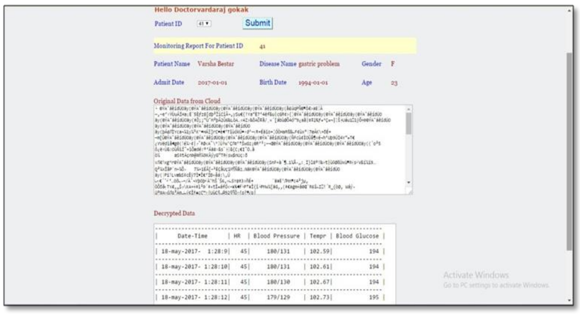

Dropbox, Inc [US] | https://www.dropbox.com/home?preview=pat_42.txt
pat_42.txt
Modified on May 31

Fig -2: Encrypted data in cloud


Hello Doctorvardaraj gokak
Patient ID
41
Submit
Activate Windows
Go to PC settings to activate Windows.

Monitoring Report For Patient ID 41

Patient Name Varsha Bestar Disease Name gastric problem Gender F

Admit Date 2017-01-01 Birth Date 1994-01-01 Age 23

Original Data from Cloud

Decrypted Data

```
-------------------------------------------------------------------
|      Date-Time       | HR | Blood Pressure | Tempr | Blood Glucose |
-------------------------------------------------------------------
| 18-may-2017-  1:28:9|  45|     180/131    | 102.59|          194 |
-------------------------------------------------------------------
| 18-may-2017- 1:28:10|  45|     180/131    | 102.61|          194 |
-------------------------------------------------------------------
| 18-may-2017- 1:28:11|  45|     180/130    | 102.67|          194 |
-------------------------------------------------------------------
| 18-may-2017- 1:28:12|  45|     179/129    | 102.73|          195 |
```

Fig -3: Encrypted and Decrypted form of data

The performance analysis between the IBKEM and QKD scheme is done and is shown in the table 1. Both the schemes are compiled and the execution timing is noted down showing that IBKEM takes less execution timing than the QKD.

Table -1: Performance Analysis of IBKEM and QKD

	IBKEM	QKD
Key Distribution	390 ms	1502 ms
Encryption	874 ms	2081 ms
Decryption	118 ms	702

6. CONCLUSION

Security and privacy of the data exchanged is most important. The data is sent securely from one place to another place with the new scheme called as Identity Based Key Encapsulation mechanism (IBKEM). The new scheme used in the patient monitoring system the patient records are securely sent to the doctor and the records are stored in the cloud in the encrypted format by using type of attributed based encryption called Cipher text policy attribute based encryption. Thus the IBKEM provides confidentiality of the data and anonymity is maintained by the Id given to each one of them. The other scheme called QKD is used to compare the execution time with the present scheme used and the result show that the IBKEM takes less execution timing than the QKD. Thus the new scheme is best suited for the secure data transfer using cloud.

REFERENCES

[1] Thaier Hayajneh , Bassam J Mohd , Muhammad Imran , Ghada Almashaqbeh and Athanasios V. Vasilakos ," Secure authentication for remote patient monitoring with wireless medical sensor network", mdpi article ,volume 16: march 2016.

[2] Rupesh Kumar Sinha , Dr. Mrinal Mishra ,Dr. S.S. Sahu "Quantum key distribution :BB84 protocol in C", IJEECS, volume 6 issue 1, January 2017.

[3] Wei Wang, Peng Xu, and Laurence Tianruo Yang, ”One pass anonymous key distribution in batch for secure real time mobile services”, IEEE conference on mobile sevices, 2015.

[4] Michel Abdalla, Dario Catalano, and Dario Fiore ,“Verifiable random functions: Relations to identity based key encapsulation and new constructions”, Springer: journal of cryptography, May 2013.

[5] Tatsuaki Okamoto, “Cryptography based on bilinear maps”, link.springer.com.

[6] Roszelinda Khalid, Zuriati Ahmad Zukarnain, Zurina Mohd Hanapi and Mohamad Afendee Mohamed, “Authentication mechanism for cloud network and its fitness with quantum key distribution protocol – a survey”, Journal of Theoretical and Applied Information Technology, Nov 2015.