International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

Private and Secured data Transmission and Analysis for Wireless Ad-hoc Network

Shrikant Kadam[1], Pramod Lad[2], Devendra Vavekar[3]

[1,2,3] *Students, DEPT. of Computer Engineering ISB&M School of Technology, Maharashtra, India*

Abstract - *A lot of work has been done to secure sensitive data. The existing solutions can protect the organizational data during transmission, but cannot stop the inside attack where the administrator of the organizational database reveals the sensitive data. We propose a practical approach to prevent the inside attack by using multiple data servers to store data by securely distributing the data onto multiple data servers. These contributions are essentially different from the solution, which relies on the Sharemind system for data analysis without considering the collusion of data servers to preserve the privacy of the organizational data in statistical analysis .We propose some new privacy-preserving statistical analysis protocols on the basis of the Paillier and ElGamal cryptosystems. These protocols allow the user to perform statistical analysis on the data without compromising the data privacy.*

The development of Privacy Protection for organizational database was motivated by business applications; today such networks are used in many organizational, educational and consumer applications, such as business process monitoring and control, and so on.What has received less attention, however, is the critical privacy concern on information being collected, transmitted, and analyzed. Such private information may include payload data transmitted through the network to a centralized data processing server.

To keep the privacy of the user's data, we proposed a new data collection protocol which splits the user's data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the user's data can be preserved. For the legitimate user e.g. receiver to access the user's data, we proposed an access control protocol, where three data servers cooperate to provide the user with the user's data, but do not know what it is

***Key Words*: : Encryption, Cyphertext, and Pillier cryptography**

1. INTRODUCTION

The development of Privacy Protection for organizational database was motivated by business applications; today such networks are used in many organizational, educational and consumer applications, such as business process monitoring and control, and so on.What has received less attention, however, is the critical privacy concern on information being collected, transmitted, and analyzed. Such private information may include payload data transmitted through the network to a centralized data processing server.

Our objective is: Protect the user data during transmission .Reliable data transmission, node mobility support and fast event detection. Timely delivery of data, power management, node computation and middleware.

Stop the inside attack where the administrator of the user database reveals the sensitive information of users.The existing solutions can protect the data during transmission, but cannot stop the inside attack where the administrator of the organizational database reveals the sensitive user data. In this, we propose a practical approach to prevent the inside attack by using multiple data servers to store data. The main scopes is securely distributing the data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistical analysis on the data without compromising the information privacy. The solution can protect the data privacy as long as the number of the compromised data servers is at most one. The data privacy can be preserved as long as at least one of three data servers is not compromised. Even if two data servers are compromised but one data server is not compromised, our solution is still secure.

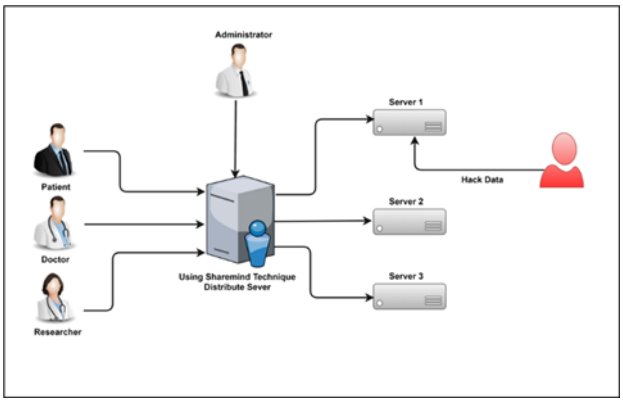
2. SYSTEM ARCHITECHTURE

Like most of the application with wireless sensor network,our architecture has four system as follows

A wireless ad-hoc network which sense the user data and transmit user data to user database system

A user data access control system which is used by the user To access the user data and to monitor it.

User data analysis system which is used by the user to query the user database system and analyze the user data statically.



System Architecture

3. PROPOSED ALGORITHM

Paillier Public-Key Cryptosystem: It is composed of key generation, encryption and decryption algorithms as follows.

Step 1: Key generation The key generation algorithm works as follows.

Choose two large prime numbers p and q randomly and independently of each other such that

gcd(pq,(p-1)(q-1))=1

Compute
N=pq,=lcm(p-1,q-1)

Where lcm stands for the least common multiple.

Select random integer g where and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:

where function L is dined as

L(u)=(u-1)/N

Note that the notation a/b does not denote the modular multiplication of a times the multiplicative inverse of b but rather the quotient of divided by b

The public (encryption) key pk is (N,

The private (decryption) key sk is (,).

If using p,q of equivalent length, one can simply choose

where N = pq and(N)=(P-1)(q-1)

Step 2:Encryption:.

Plaintext data convert into cipertext form

Step 3: Decryption:

Let c be the ciphertext to decrypt, where the ciphertext

step 4: Homomorphic Properties A notable feature of the Paillier cryp tosystem is its homomorphic properties. Given two ciphertexts The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,An encrypted plaintext raised to a constant k will decrypt to the product of the plaintext and the constant,However, given the Paillier encryptions of two messages, there is no known way to compute an encryption of the product of these messages without knowing the private key

4. RELEVENT MATHEMATICS

Let W be the whole system which consist

W= IP, PRO, OP

Where. **IP is the input of the system.**

A) IP= P, SD, SN, PD, U

1. P is the number of users in the system.
2. SN is the set of number of sensing nodes in the system.

3. SD is the sensing data sensed from the information SD.

4. PD is the users database system which consists of number databases.

5. U is the set of number of user in the systems that are accessing the data from user database server.

B) **PRO is the procedure of our proposed system:**

Step 1: At first the wireless medical network which senses the patient's body and transmits the users data to a users database system.

Step 2: A user's database system which stores the users data from distributed and provide squaring services to users.

Step 3: A users data access control system which issued by the user (e.g., physician) to access the users data and monitor the users.

C) OP is the output of the system: OP is the output of the system

The system provides the privacy to the users sensible data available on the users database system in the sense of inside attacks.

5. CONCLUSIONS

We have investigated the security and privacy issues in the wireless network data collection storage and queries and presented a complete solution for privacy-preserving wireless network. To secure the communication between user and data servers.

To keep the privacy of the user's data, we proposed a new data collection protocol which splits the user's data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the user's data can be preserved. For the legitimate user e.g. receiver to access the user's data, we proposed an access control protocol, where three data servers cooperate to provide the user with the user's data, but do not know what it is.

REFERENCES

[1] Xun Yi, AthmanBouguettaya, DimitriosGeorgakopoulos, Andy Song and Jan Willemson "Privacy Protection for Wireless Medical Sensor Data", in proc. IEEE Transactions on Dependable and Secure Computing, 2015.

[2] In Proc. ESORICS'08, pages 192-206D. Bogdanov, S. LaurSharemind: a Frameworkfor Fast Privacy-Preserving Computations

[3] Wood, A.; Virone, G.; Doan, T.; Cao, Q.; Selavo, L.; Wu, Y.; Fang, L.; He, Z.; Lin, S.; Stankovic, J. ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring; Technical Report CS-2006-01; Department of Computer Science, University of Virginia: Charlottesville, VA, USA, 2006.

[4] Cryptography And Network Security from William Stallings. Reference 4.