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

PRIVATE AND SECURE DATA TRANSMISSION AND ANALYSIS FOR WIRELESS AD-HOC NETWORK

Prof. Sonali Khairnar[1], Pramod Lad[2], Devendra Vavekar[3] , Shrikant Kadam[4]

[1] *Sr. Professor, Department of Computer Engineering, I.S.B.&M. School Of Technology Pune, Maharashtra, India*
[2,3,4] *B.E. Student, Department of Computer Engineering, I.S.B.&M. School Of Technology Pune, 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 are proposing approach to prevent the inner 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 Share mind system for data analysis without considering the collusion of data servers to preserve the privacy of the organizational data. We are proposing some new privacy-preserving analysis protocols on the basis of the cryptosystem developed by Paillier and ElGamal. These protocols allow the user to perform statistical analysis on the data without compromising the data privacy. 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. 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: **Cypher-text, Privacy-Preservation, Ad-hoc Network, etc.**

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. This kind of 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 system, we are proposing a practical approach for the prevention of 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 ARCHITECTURE

Before 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.

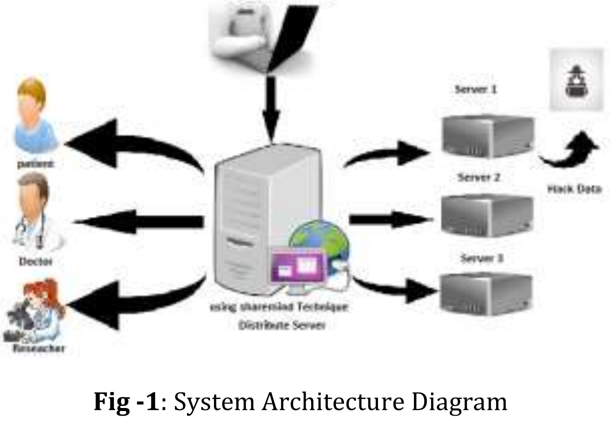

Fig -1: System Architecture Diagram

3. MATHEMATICAL MODEL

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 user database system which consists of 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 data and transmit to database system.
Step 2: A user database system which stores the users' Data. Step 3: A user's 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. The system provides privacy to the user's sensible data

4. 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 PQ of equivalent length, one can simply choose

Where, N = PQ and (N) = (P-1) (Q-1)

Step 2: Encryption:

Plaintext data convert into cipher text form

Step 3: Decryption:

Let c be the cipher text to decrypt, where the cipher text

Step 4: Homomorphic Properties a notable feature of the Paillier crypto system is its homomorphic properties. Given two cipher texts The product of a cipher text with a plaintext raising g will decrypt to the sum of the corresponding plain texts 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.

4.1 AES Algorithm.

AES is an iterative rather than Festal cipher. Its working is based on 'substitution and permutation network'. It is comprises of a series of linked operations, some of which involve replacing inputs by the specific output (substitutions) and others involve shuffling bits around (permutations). AES algorithm performs all its operations on bytes rather than bits. AES algorithm treats the 128 bits of a plaintext data block as 16 bytes data. These 16 bytes data are arranged in the four columns and the four rows for processing as a matrix unlike DES, the number of rounds in AES is variable and it depends on the length of the key. AES algorithm uses 10 rounds for 128-bit keys and 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES algorithm key.

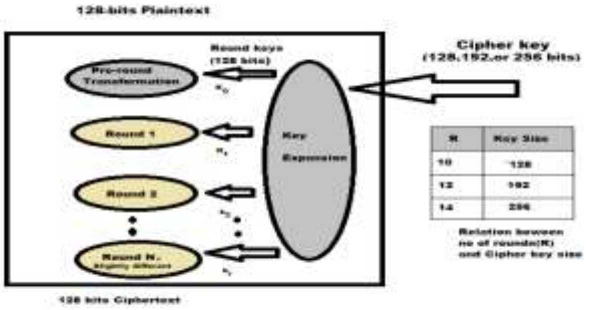

Fig -2: AES Algorithm

5. RESULT

The project is implemented as prototype model. we used database as a different servers. We use a text file for transmit the data. The text file which contains data has been successfully transmitted. The data is encrypted by the encryption algorithm it is divided into three parts and stored on three different places on the database. While accessing the data the data is merged and decrypted and complete data is accessed by the user. This is the prototype model, suppose we performed operation on a text file which contains following data.

"Data security is very important for the commercial organizations."

When we send above data it will encrypt and store on three different locations. Following table shows the operations.

ORIGINAL DATA	SERVER 1	SERVER 2	SERVER 3
Data security is very important for the commercial organizations	d7o4cc7df51885cgs	g0ader3on7f84lsk0v4t7	Xffc852oh7dg85c

Table1. Result

The above table shows the result. Colum 1 shows the original data and remaining column's shows the encrypted data that is divided and stored on three different columns.

6. CONCLUSIONS

We have investigated the security and privacy issues in the network data collection storage and queries and presented a complete solution for privacy-preserving 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, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson "Privacy Protection for Wireless Medical Sensor Data" in proc. IEEE Transaction.

[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.\

[5] Chen, B.R.; Peterson, G.; Mainland, G.; Welsh, M. LiveNet: Using Passive Monitoring to Reconstruct Sensor Network Dynamics. In Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor System (DCOSS'08), Santorini Island, Greece, 11–14 June 2008.

[6] Dimitriou, T.; Loannis, K. Security Issues in Biomedical Wireless Sensor Networks. In Proceedings of 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies (ISABEL'08), Aalborg, Denmark.

[7] A. Sawand, S. Djahel, Z. Zhang and F. Nait-Abdesselam, "Toward Energy Efficient and Trustworthy Ehealth Monitoring System," China-Commun.,vol.12, No.1,pp.46-65,Jan 2015

[8] C.Wang, B. Zhang, K. Ren, J.M. Roveda "A Privacy-Aware Cloud-Assisted Healthcare Monitoring System" in.Proc. of 33rd IEEE INFOCOM, 2014,pp.2130-2138.

BIOGRAPHIES

1'st Author Photo

Prof. Sonali Khairnar Sr. Professor, Computer Engineering Department, I.S.B.&M. School of Technology Pune.

2nd Author Photo

Pramod Lad Student, Computer Engineering Department, I.S.B.&M. School of Technology Pune

3rd Author Photo

Devendra Vavekar Student, Computer Engineering Department, I.S.B.&M. School of Technology Pune

4th Author Photo

Shrikant Kadam Student, Computer Engineering Department, I.S.B.&M. School of Technology Pune