A Secure and Privacy Preserving Technique in Distributed Information Sharing using AES Encryption and Genetic Algorithm

Dharani.M
PG Scholar
Department of Computer Science and Engineering
Nandha college of Technology
Erode.
dharanimurugasamy62@gmail.com

R.Vidhya
Assistant Professor
Department of Computer Science and Engineering
Nandha college of Technology,
Erode.

Abstract: In many organizations distributed information sharing is used to share data in a large network. In distributed Information sharing there are many chances to hack the technical and personal information of client and server in a network. Earlier Information Brokering methods are used where brokers are used to share the information among the clients and servers. This approach has a drawback where the brokers cannot be trusted to share information. In this paper we propose a technique to preserve the security and privacy of the distributed network where information is shared. We also use a shared medium as an interface between the server and client. AES encryption is used to encrypt the information in server which is to be sent to the client. In shared medium we use Digital Signature Algorithm to perform client authentication to send the information to the requested client. Genetic Algorithm is another technique which is used to detect the attackers who tries to hack the information in shared medium. Since we use two cryptographic techniques the security maintained will be high. Use of Genetic Algorithm also enhances the security measures of the system and it will be difficult for attackers to hack the information easily. We use the above three techniques to improve the performance measure.

Keywords--Security, AES Encryption, Genetic Algorithm, Network, Attackers.

I. INTRODUCTION

Distributed Information Sharing is where many servers and many clients can share information with each other in a single network. Now-a-days in all the organizations and companies they implement distributed information sharing or distributed information system where many servers and many clients are connected with each other. Since a single organization have many branches which can be said as client.[9] So a single server is used to control all the clients and process the requests sent by those clients. Server will send the information requested by client through the network. There will be many disadvantages as the time taken for a client to receive information will be higher, as each client has to wait to access the information from the server when some other client is using the server. If the attacker attacks the server it will lead to the destruction of entire networks.

To overcome these difficulties we use distributed information sharing system where many servers will be connected with many clients to reduce the processing time of each client in a network and if any attacker tries to attack a particular server, the network can be recovered using the other servers. In this distributed information sharing also we have threat of attackers which may attack the information which will be shared among the server and client in a network.[3] To avoid this problem we can use some security mechanisms to secure the information from the attackers. In a network, information can be secured using cryptographic techniques.

II. CRYPTOGRAPHY

Cryptography is a technique which is used to secure the information sent from server to client in a network. As we mentioned earlier in distributed network there will be many security problems. So to avoid these problems we use cryptographic techniques which is difficult for the hackers to attack the data and the identity of client and server in a network. The information sent from a server to the client will be converted to a secret form or any secret code will be added which cannot be identified by any attackers. In cryptography we have two main techniques namely encryption and decryption. Encryption is where the information is converted into a secret form which is to be sent to the client from the server side.

Decryption is where the converted secret information will be retrieved as original information in the client side. In modern cryptography there are two main types: Symmetric cryptography and Asymmetric cryptography. Symmetric cryptography is where encryption and decryption share a single or common key between server and client. In asymmetric encryption public and private keys are used for encryption and decryption in server and client side respectively.

III. EXISTING SYSTEM

In existing system, distributed system uses brokers for sharing the information in the network.[1] In this data sent will not be encrypted and no cryptographic techniques are used for security.

A. Automaton Segmentation

Automaton Segmentation is to logically divide the global segment into multiple independent segments and physically divide the segment into different brokering components.

B. Query Segment Encryption

In this method we use two encryption postencryption and preencryption. Query segments are processed by a set of coordinators along a path in the coordinator tree. Each query is encrypted using the public key of the coordinator. Postencryption is necessary for the remaining coordinators in later processing. In this they also used cumulative encryption which is used to process the descendent or self axis.

C. Privacy Preserving Query Brokering Scheme

In this scheme they proposed four phases:[6]

1. A user needs to authenticate to join the system with the local broker. A user submits an XML query with each segment encrypted by the public keys and session keys.
2. Broker prepares a metadata which retrieves the role of authenticated user and creates a unique ID.
3. After receiving the encrypted query, the above two techniques automaton segmentation and query encryption to perform access control and query routing.
4. Data server receives a query in encrypted form. After decryption the data server evaluates the query and returns the data.

In existing system key has to be maintained and broker's information has to be updated regularly whether they leave the system or join the system. Maintenance is also needed for the metadata which is formed in the second phase.[4]

Since brokers are used security will be very less. Brokers are not trusted all the time. Sometimes brokers will share information with the attackers. The data sent will not be encrypted. Original data sent will be hacked easily.

IV. PROPOSED WORK

A. Genetic Algorithm

Genetic Algorithm (GA) is a search heuristics which is used to solve the optimization and search problems. It solves the problem using various methods such as inheritance or selection, mutation, crossover. Initially many individual solutions are produced using initial population. Using selection method a breed of generation is produced. Fitness function is used in the selection method to select the necessary solution. After selection process other two processes crossover and mutation are implemented. [2]

Algorithm for Genetic Algorithm:

i. choose initial population

ii. evaluate each individual's fitness

iii. determine population's average fitness

iv. repeat

   a. select best-ranking individuals to reproduce.
   b. mate pairs at random.
   c. apply crossover operator.
   d. apply mutation operator

e. evaluate each individual's fitness

v. determine population's average fitness.

vi. until terminating condition.

In this paper, genetic algorithm is used for detecting the hackers in the network. Client ID is converted into a secret form using genetic algorithm and it is stored in the database. When client requests data from sender, the shared medium will verify the client with the stored ID's and then connection will be made between server and client. If it is not the ID then it will be declared as a hacker and permission will be ignored to make connection with the server.

B. *AES Encryption*

AES encryption is a symmetric cryptography and based on a substitution permutation network. It is fast in both software and hardware when compared to other encryption techniques. In many real time applications AES encryption is used. In AES we use a 128 bit plaintext and key size will be of 128 bit. We use 10 rounds of encryption and decryption. [16]

In each round we have four operations: sub bytes, shift rows, mix columns and add round key. Initially add round key operation is performed. In other rounds the four operations are performed in the order respectively. In final round mix column operation is not performed.

Decryption process is vice-versa of encryption mechanism. In decryption the same keys are used which are used in the encryption.

In this paper we use AES Encryption in server side to encrypt the data to be sent to the client. The data will be split into packets and it will be encrypted. The encrypted data will be sent to the client through shared medium. Encrypted data will be in a secret form which cannot be identified by any attackers.[10] This is used to maintain the security in the distributed network while sharing information with other clients and server.

C. *Digital Signature Algorithm*

Digital Signature Algorithm (DSA) is an authentication algorithm used to process the Digital Signature. Digital Signature is to check the validity of the user. It is also used in variety of applications to ensure the integrity of data exchanged or stored and to prove the recipient and originator. It is used in open network. Digital Signature is public-key cryptography where we use both private and public key. In Digital Signature Algorithm we have three main phases: key generation, signing, verifying. Digital Signature is used with the encryption technique to enhance the security.[11]

We use hash algorithm to calculate the keys and produce a value for signing the encrypted data. Once a sign is made then the sign will not be repeated for other encrypted data. The algorithm parameters used will not be shared with other user. Public and private keys are generated which can be shared with other user.

In this paper, when information is encrypted and signed it will be sent from the server to client through shared medium. In shared medium before forwarding the data to the client it will verify the signature with the client using the keys generated and if the sign is verified then data will be sent to the client. This will maintain the privacy of the user. No other user can hack the data from the server easily.

D. *System Architecture*

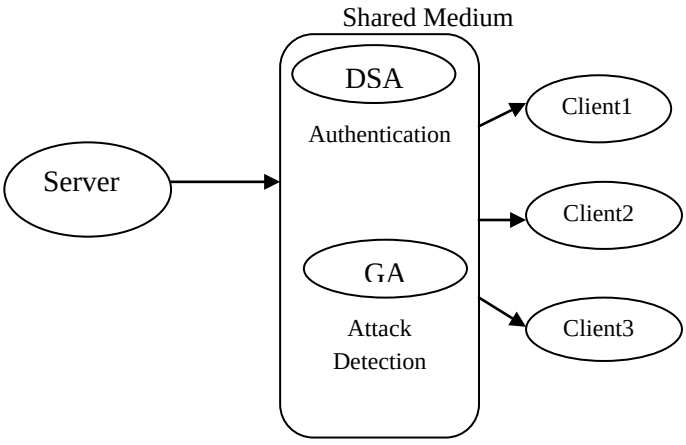

Fig.1. System Architecture

V. IMPLEMENTATION

In many places while using distributed information sharing security is less and recipient and originator's identity can be denied. To avoid these problems in this paper we propose a novel approach using the above three techniques to implement the security and integrity. When security is implemented the data will be secured from the hackers and using integrity the server and client identity is verified.

The mechanism can be implemented in both server and client side. In server side, the information to be sent is split into packets and each packet is encrypted using AES Encryption. Server, Shared medium and Client are connected with each other using IP address. The clients connected will be verified by the shared medium.

The information encrypted is sent to the shared medium for authentication. When information is received by the shared medium it checks the authentication of client to forward the information. Once the authentication is checked, the information will be sent to the client. Authentication will be verified by the Digital Signature Algorithm.

Information sent to the client will be downloaded in the client side and retrieved by the user. The data sent will be in an encrypted form so it is decrypted in client side using AES Encryption.

VI. CONCLUSION

In this paper we analyzed security and privacy problems in distributed information sharing or distributed networks and proposed a new mechanism using Genetic Algorithm, AES Encryption and Digital Signature Algorithm. The data sent in a network is secured using AES Encryption and Privacy is maintained using Digital Signature Algorithm.

We also detect the hackers who try to attack the data in a network using Genetic Algorithm. Since we use AES Encryption the security process will be fast and more secure. We also use Genetic Algorithm which cannot be hacked easily by any hackers to retrieve the client ID. Our analysis shows that performance and security will be high for sharing information in a distributed network.

REFERENCES

[1] Fengjun Li, Bo Luo, Peng Liu Dongwon Lee and Chao-Hsien Chu, "Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing", IEEE Transcations On Information Forensics And Security, 2013.

[2] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, "An Implementation of Intrusion Detection System Using Genetic Algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[3] Dawn Xiaodong Song David Wagner Adrian Perrig," Practical Techniques for Searches on Encrypted Data", Security and Privacy, 2000. S&P 2000, Proceedings. 2000 IEEE Symposium.

[4] Li F, Luo B, Liu P, Lee D, Mitra P, Lee W, and Chu C, "In-broker access control: Towards efficient end-to-end performance of information brokerage systems", in Proceeding IEEE SUTC, Taichung, Taiwan, pp. 252–259, 2006.

[5] Luo B, Lee D, Lee W C and Liu P, "Qfilter: Fine-grained runtime XML access control via NFA-based query rewriting enforcement mechanisms", in Proceeding CIKM, pp. 543–552, 2004.

[6] Zhiqiang Yang, Sheng Zhong, and Rebecca N. Wright, "Privacy-Preserving Queries on Encrypted Data", In Proceedings of the 11th European Symposium On Research In Computer Security (Esorics), 2006.

[7] Stoica I, Morris R, Liben-Nowell D, Karger D, Kaashoek M, Dabek F, Balakrishnan H, "Chord: A scalable peer-to-peer lookup protocol for Internet applications," IEEE/ACM Transaction on Networks, volume. 11,no. 1, pp. 17–32, February, 2003.

[8] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan, "CryptDB: Protecting Confidentiality withEncrypted Query Processing",2011 ACM Transaction.

[9] Nickolai Zeldovich, Silas Boyd-Wickizer, and David Mazi`eres," Securing Distributed Systems with Information Flow Control", 5th usenix symposium on network systems design and implementation,2008.

[10] Alan Kaminsky, Michael Kurdziel, Stanisław Radziszowski," An Overview of Cryptanalysis Research for the AdvancedEncryption Standard", IEEE Military communications conference, 2010.

[11] Julia Juremi Ramlan Mahmod Salasiah Sulaiman Jazrin Ramli ,"Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key ", International Journal of Cyber-Security and Digital Forensics ,2012.

[12] Prakash Kuppuswamy, Peer Mohammad Appa,Dr. Saeed Q Y Al-Khalidi,"A New Efficient Digital Signature Scheme Algorithm based on Block cipher", IOSR Journal of Computer Engineering,2012.

[13] Luo B, Lee D, Lee W C and Liu P, "Qfilter: Fine-grained runtime XML access control via NFA-based query rewriting enforcement mechanisms", in Proceeding CIKM, pp. 543–552, 2004.

[14] Stoica I, Morris R, Liben-Nowell D, Karger D, Kaashoek M, Dabek F, Balakrishnan H, "Chord: A scalable peer-to-peer lookup protocol for Internet applications," IEEE/ACM Transaction on Networks, volume. 11,no. 1, pp. 17–32, February, 2003.

[15] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan, "CryptDB: Protecting Confidentiality withEncrypted Query Processing",2011 ACM Transaction.

[16] Wikipedia Website: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard