Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.975 – 977

RESEARCH ARTICLE

Detection of Guilty Agent using Encryption Algorithm and MAC Address

Maulik Bhagat[1], Prof. G. B. Jethava[2]
[1]PIET, Waghodiya
[2]PIET, Waghodiya
[1st] mauliklcl@gmail.com, [2nd] g.jethava@gmail.com

Abstract--- There are many websites that publish information and provide access of information on the internet. All that websites has many different web application programs that contains potential information or data that have to be protected. In many organizations, business scenarios and company outsource its data to the other company or organization or agents, all these agents are known as trusted third party agents. The data owner give the confidential data to the trusted third party agents and their possibility that any of that trusted agent can leak the potential data. It is mandatory to detect the guilty agent, who leaks the data to unauthorized agents. For identification of leaked data in existing system uses watermarking technique and data allocation strategies with adding fake objects. However, it has deficiency is that watermarking data can be modified or change. In proposed system uses AES algorithm for encryption of requested data. As a result, unauthorised party is unable to view or access the confidential data. One more technique used for improving chances of detecting guilty agent is MAC (Media Access Control) address.

Keywords---Data Leakage, Data Allocation Strategies, Guilt Agent, Confidential Data, AES algorithm

I. INTRODUCTION

A company, business, organization, all have their confidential data. And these data such as customer details, patient records, credit card details, finance information. All these kind of data must be protected. Sometimes company have to share that data to the trusted third party agents for surveying, improving, research etc. At that time security of that data is a major question. If any agent from them will leak the confidential data, it leads a greatest financial loss. So, it is a need to provide the confidentiality of the data and identify the guilty agents, which are from the trusted agents, who leak the data to unauthorized person. For improving the chances of identifying guilty agents, another new technique has been proposed. This technique will use the MAC address and AES algorithm. The MAC address improve the chances of identifying guilty agents. And AES algorithm will encrypt the requested data by the agents.

II. PROBLEM STATEMENT

Data leakage is defined as unintentional or accidental distribution of private or sensitive data to an unauthorized party. Detection of leaked data and guilt agent is major challenge in many industries. To overcome the problems many techniques have been invented to identify guilt agent and leaked data. But, still the issue are not completely solve. There has to be some new and advance approach or technique to efficiently identify the guilt agent.

III. RELATED WORK

Detection of data leakage can be done using various technique such as perturbation, water marking, K-Anonymity, M-Score technique. But it has some limitations such as:
In watermarking technique, it involve some modification of the original data and sometimes watermark scan can be destroyed if the data recipient is malicious. K-anonymity technique is only used for storing purpose not for processing purpose. And it doesn't consider the diversity of the sensitive attribute value. M-Score technique is assigns the score depending on the sensitivity level of the data.

IV. AES (ADVANCED ENCRYPTION STANDARD) ALGORITHM

AES (Advanced Encryption Standard) algorithm is a symmetric block cipher. It is best algorithm for security purpose. AES does not uses a fiestel structure. Instead, each full round consist of four separate functions: Byte substitution, Permutation, Arithmetic operation and XOR with a key. It uses 128 bit for block size and 128, 192 or 256 bits for key size.

Four different stages are used: One of Permutation and other three for Substitution.

- Substitution byte: Uses an S-box to perform byte-by-byte substitution of the blocks.
- Shift rows: A simple permutation.
- Mix Columns: A substitution that makes use of arithmetic over GF(28).
- Add Round key: A simple bitwise XOR of the current block with a portion of the expanded key.

V. MAC (MEDIA ACCESS CONTROL)

A MAC (Media Access Control) is a unique identifier assigned to network interfaces for communications on the physical network segment. Each and every computer has a unique MAC address for its Ethernet, Modem, Wireless network card. Each and every network devices have a unique different MAC address. Mac address contains numbers and letters. Numbers from 0 to 9 and letters from A to F. Such as, 00:0E:84:27:3D:E7 . In this system MAC address is used for detecting the guilty agent. If agents MAC address mismatch with stored MAC address then it will be a guilty agent..

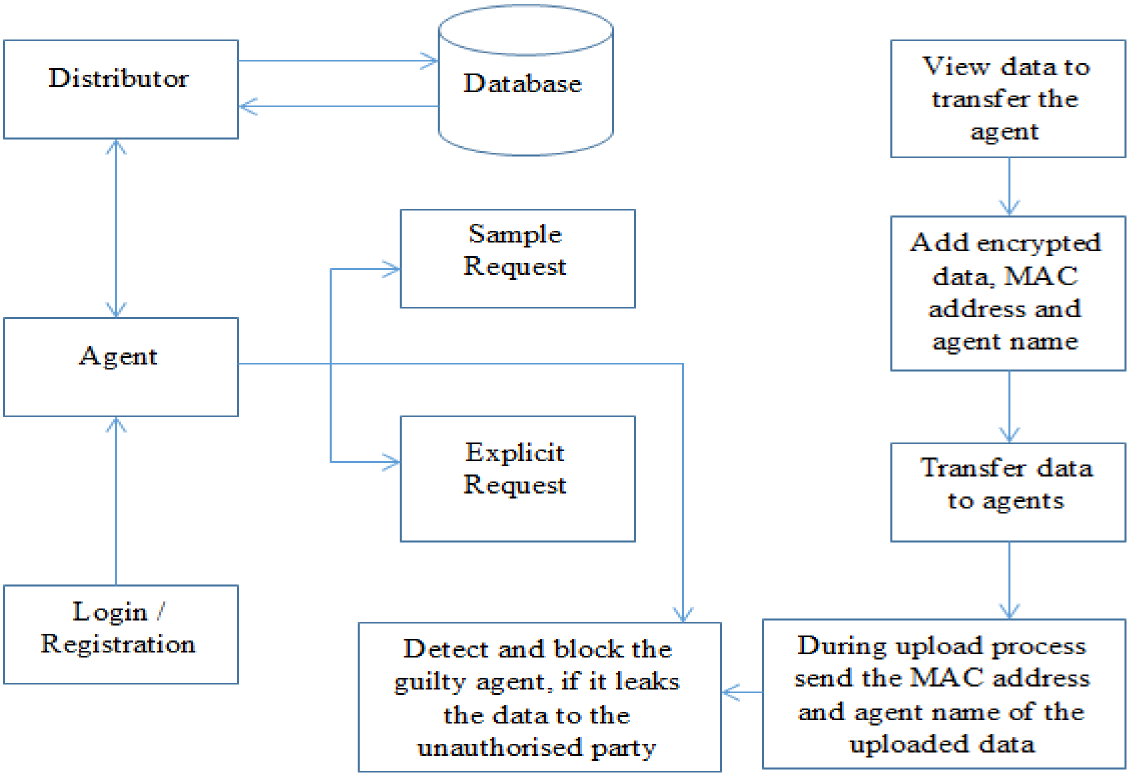
Distributor
Database
View data to transfer the agent
Sample Request
Add encrypted data, MAC address and agent name
Agent
Explicit Request
Transfer data to agents
Login / Registration
Detect and block the guilty agent, if it leaks the data to the unauthorised party
During upload process send the MAC address and agent name of the uploaded data

Fig 1. Proposed System

Implementation Methodology:

Step 1: The authorized agent should fill the registration form. The registration form have all the information of the agent. And when it submits the form, System will take the MAC address of agent automatically.

Step 2: The admin is known as distributor. The distributor can approve or cancel the request of the agent. If request is accept, then agent can send the request for data.
Step 3: After getting request for the data. The distributor will send the requested data to the agent with encrypting the data using AES algorithm. The encrypted data has the requested data, MAC address and username. The data is encrypted with secret key.
Step 4: Only authorized agent is able to decrypt the data on the server side by checking agent's MAC address with stored MAC address. It will also check the authority of the agent before decryption of data.
Step 5: The authorized agent is unable to copy or modify the data.
Step 6: If authorized party leaking the data to the other, then unauthorized agents are not able to access that data, because it is encrypted.
Step 7: If unauthorized agent wants to decrypt the data, it should upload data. Upload data contains agent's username. And before uploading data on server side, system checks MAC address of the agent. If MAC address is different , than it identifies guilty agent.
Step 8: The trusted agent can decrypt and process the data, because it has authority. So, from this system improve the chances of identifying guilty agent.

VI. CONCLUSION

In organization, most of their potential data is shared to the trusted third party. But, they cannot assured that agent is loyal. So the desired objective of the distributor is to detect the guilty agent who leak the data. Thus, this system can identifies the guilty agent using MAC address and AES Encryption algorithm without adding fake object and without calculating guilt probability. While the AES algorithm is used to encrypt the potential data. So unauthorized agent is unable to access the confidential data. And MAC address is used to identify the guilty agent. So, this system used to identify the guilt agent by providing the privacy of data.

ACKNOWLEDGEMENT

For all the efforts behind the paper, I first & foremost would like to express my sincere appreciation to the staff of Dept. Information Technology for their extended help & suggestions at every stage of this paper. It is with a great sense of gratitude that I acknowledge the support, time to time suggestions and highly indebted to my guide HOD Prof. G. B. Jethava. Finally, I pay sincere thanks to all those who indirectly and directly helped me towards the successful completion of the paper.

REFERENCES

[1] Panagiotis Papadimitriou, Hector Garcia-Molina, *A Model for Data Leakage Detection* Stanford University.
[2] Panagiotis Papadimitriou, Hector Garcia-Molina, *Data Leakage Detection* IEEE Transaction on Knowledge and Data Engineering, Vol-23,No 1, January 2011 pp. 51-63
[3] Ajay Kumar, Ankit Goyal, Ashwini Kumar, Navneet Kumar Chaudhary, Sowmya Kamath ,*Comparative Evaluation of Algorithms for Effective Data Leakage Detection*, IEEE Conference on Information and Communication Technologies (ICT 2013), pp. 177-182.
[4] Anush Koneru, G.Siva Nageswara Rao, J. Venkata Rao, *Data Leakage Detection Using Encrypted Fake Objects*, International Journal of P2P Network Trends and Technology Vol-3 Issue-2 2013 pp. 104-110
[5] B. Sruthi Patil, Mrs. M. L. Prasanthi, *Modern Approaches for Detecting Data Leakage Problem*, , International Journal Of Engineering And Computer Science, Vol-2, Issue-2, Feb 2013 pp. 395-399.
[6] Jaymala Chavan, Priyanka Desai, *Relational Data Leakage Detection using Fake Object and Allocation Strategies*, International Journal of Computer Applications, Vol-80, No.16 , October 2013 pp. 15-21.
[7] Rudragouda G Patil, *Development of Data leakage Detection Using Data Allocation Strategies*, International Journal of Computer Application in Engineering Sciences Vol-1, Issue-2, June 2011 pp. 197-200.
[8] Sandip A. Kale, Prof. S. V. Kulkarni, *Data Leakage Detection*, International Journal of Advanced Research in Computer and Communication Engineering Vol-1, Issue-9, November 2012 pp. 668-678
[9] Jagna Ajay Kumar, K. Rajani Devi, *An Efficient And Robust Model For Data Leakage Detection System*, Journal of Global Research in computer Science, Vol-3, No-6, June 2012 pp. 91-95
[10] *Chapter 2 Data Leakage* http://www.springer.com/978-1-4614-2052-1