RESEARCH ARTICLE OPEN ACCESS

Data Leakage Detection in Network Using the Passive IP Trace back (PIT) Technique

S.Babu[1] , V.Aswini[2]

[1,2] (Department of CSA, SCSVMV UNIVERSITY Enathur, Kanchipuram)

Abstract:

Data leakage is the transmission of data or information from an organization to unauthorized parties. Data leakage means distribution of private or sensitive data to an unauthorized user. Private data of an organization includes financial information, employee's personal information and other confidential information related to an organization. Sometimes private data may transmit to trusted third person. This will automatically increase the possibilities of unnecessary data transmission. In the existing system, watermarking technique has used in order to detect data leakage. It is not possible to detect data leakage properly by using watermarking technique. In this research work, Passive IP Traceback (PIT) and embedding technique used to identify the unauthorized user and to detect the data leakage. The embedding technique uses the Enhanced Homomorphic Encryption technique for key generation. In this algorithm first, it generates the key and then encryption of the sensitive data by using key has done. The decryption key must distribute to the corresponding group member. Finally, add the fake objects for recording the behavior for guilty agent. After embedding, the user distributes the data to the group member. The group member receives the key and then user can decrypt the data by using the receiving key. The PIT algorithm detects the data leakage, if anyone redistributes the data to the outside party. It also automatically record the behavior of guilty agent, which one is send to the distributor. To analyze the performance of the proposed model, different types of text files been used in the model. The experimental result shows that, the proposed system is efficient to avoid data leakage by identifying guilty agents and it used to maintain confidential information of an organization.

Keywords- **Data leakage, Decryption, Encryption, Guilty agent, Passive IP Trackback.**

I. Introduction

In present generation, business organization, enterprise and many different sectors requires transmission of data from one place to other. Data leakage is a major problem faced by many organizations. Data leakage means the accidental or unintentional distribution private or sensitive data to an unauthorized entity. There are many data security is designed to avoid data leakage which uses different encryption techniques but still it is very hard for any system administrator to trace out all sort of data leakage in the network. This will create many ethical issues within an organization. To provide protection against various data leakage some of the widely used technologies are firewall and encryption techniques. In data leakage process, sensitive data disclosed to unauthorized user either by malicious intent or by inadvertent mistake. Private or company information, confidential information and credit card data are referred has sensitive data of an organization. Data leakage detection plays an important role in order to manage and protect confidential information. The aim of this paper is to determine the agent who leaked the data by using encryption concept. In encryption, the information is encoded a way that it can be read by authorized user only.

II. Related work:

Data leakage is very critical problem in now a day. The distributor must allocate the data to the unwanted distributor so watermarking technique used to allocate the data [1]. Data leakage detection is using two conditions namely, sample or explicit condition using to protect the data in agents [2] [4]. To detect the data leakage should be provided some security will issue to the data, using data allocation strategies to improve identify who leaks the data in unauthorized user [3] [8]. Unobtrusive techniques for data leakage detection must be identifying the guilty agents using the existing system [5]. A new model used to the allocation strategies using the new algorithm Shortest Request First (SRF) and knowledge allocation methods must protect the data leakage to the unauthorized user [6] [7]. An existing system using List Significant Bit (LSB) steganography concept different for other concept using detect the leakage [9]. A model of some online attack for computer forensics proposed to crime attack using algorithm based on data mining for association rule mining [10].

III. METHODOLOGY

a) Existing system:

In an existing system, watermarking technique has used for the detection of data leakage, which comes under technique with alternation concept. In this technique, a unique code is embedded in each distributed copy. Later if that copy is found with unauthorized party, the leaker can be identified. Initially, the original data must modify and coded message further transferred. This technique is long process and it requires modification of the original data. Furthermore, watermarks can be destroying sometimes if the data recipient is malicious

Drawbacks:

Two major drawbacks of the watermarking technique are:

1. Technique uses modification of original data. However, in some application the data must not altered. The sensitive data must be transfer without alteration.
2. Watermarks can destroy sometimes if the recipient is malicious.

b) Proposed system

In the proposed system, Passive Ip Traceback (PIT) is used for detection of data leakage and identification of guilt agent. Initially, the data distributor adds a fake objet to the entire text i.e., the original data is encrypted. The fake object is added by enhanced Homomorphic encryption for key generation. Once the sensitive data encrypted then the distributor distributes the sensitive data to the authorized parties. If any one of the authorized party forward the sensitive data to the unauthorized party then, automatically block the forwarding process and automatically identify the guilt agent. That information is then sends back to the distributor. The guilt agents are record in the guilt list. The distributor views the guilt list and comes to know about all guilt agents. The distributor automatically block the guilt agent whose is responsible for the data leakage.

c) Passive IP Traceback (PIT) Mechanism

Step 1: The user must fill the user registration form.

Step 2: The entire member in-group communicates with each other.

Step 3: The user must create a group and then view the group member details.

Step 4: The distributor must select a file in the path and encrypt the file to send the group member or anyone in the group member.

Step 5: The viewer must get a file to decrypt the data and read some message in the file.

Step 6: The group member any one must redistribute the file in another third person to detect the user using PIT mechanism.

d) Homomorphic Encryption

1. Generation of key: The Encryption of plaintext will using he pair keys like Secret Key (SK) and public key (PK).

2. Encryption: The distributor using the encryption technique keys like Secret Key (SK) and sent to the server.

3. Evaluation: The function used by the server, must being evaluate the cipher text and then performed required using public key function.

4. Decryption: The authorized user must decrypt the text using secret key and gets the original result.

e) Modules

- Data Distributor
- Sensitive data embedding
- Data Distribution
- Data Leakage detection
- Data Leakage prevention

Data Distributor:

The data distributor can form the group for allocating the work. The group members are called third party. The distributor can get the sensitive data, which is like person data, Social network raw data and so on. After getting the sensitive data then the distributor can distribute the data to the all group members.

Sensitive data embedding:

After getting, the sensitive data, which is, embed by using the Enhanced Homomorphic Encryption. In this algorithm generate the key and then encrypt the sensitive data to the by using the key. The decryption key distributed to the corresponding group member. Finally add the fake object for recording the behavior for guilty agent.

Data Distribution:

After Embedding, the data then the data distributor distribute the data to the group member. The group member receives the key and data then the user can decrypt the data by using the receiving key.

Data Leakage detection:

The PIT algorithm, must detecting the data leakage. If anyone redistribute the data to the outsider party then automatically block the forwarding request and automatically record the behavior of guilty agent, which is send to the distributor.

Data leakage prevention:

The distributor can be view the guilty agent then automatically remove the agent from the group and add the guilt agent into the guilty agent list for more data leakage prevention.

IV. RESULT AND DISCUSSION

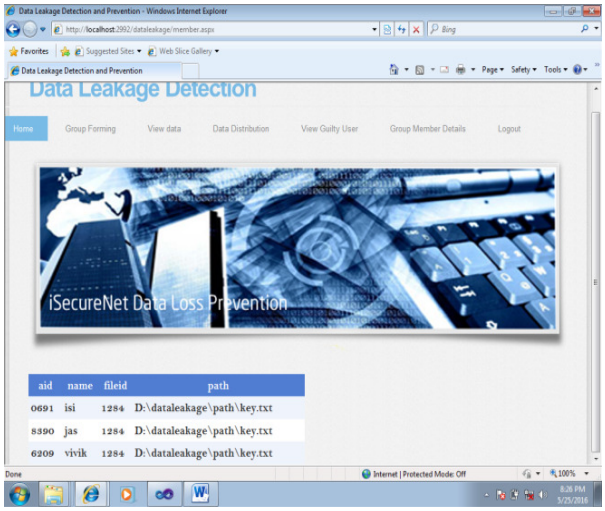

Fig 4.1 generates the key and then encrypts the sensitive data by using the key.

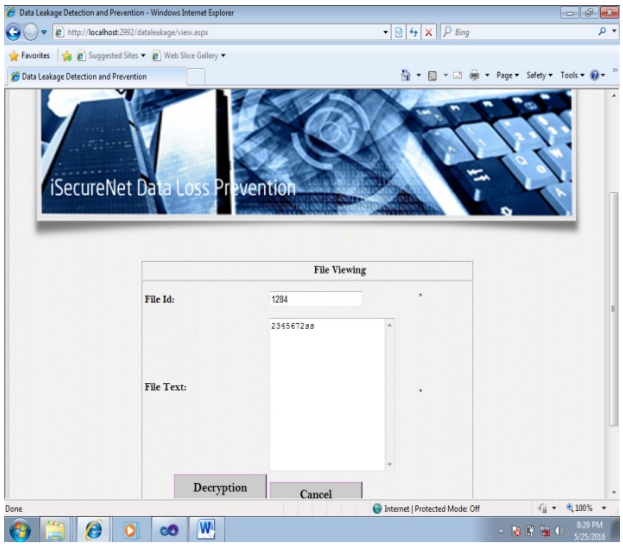

Fig 4.2 PIT algorithm for detecting the data leakage.

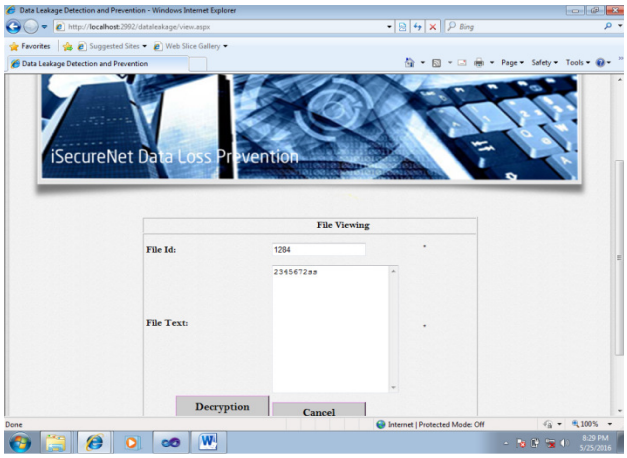

Fig 4.3 The distributor can be view the guilty agent.

V.CONCLUSION

In this work, the problems raised while transferring sensitive data from one distributor to multiple trusted agents. The transmission of data process generally, has done only among authorize parties. Some of the party may leak the data to unauthorized party. Detecting the guilt agent and block them is the major goal in this work. The purpose to block the guilt agent is that, the sensitive data that must keep confidentially. It is not easy to detect the guilt agent. Passive IP Traceback is used for guilt agent detection. Enhanced Homomorphic encryption used for preventing data leakage that provides the user must secure to our data using data security. When the data is leak to unauthorized party, distributor can able to identify the guilt agent by checking guilt list. It is supposed to block that guilt agent before transferring data further. In this way, a guilty agent is identified and data leakage prevented.

VI. FUTURE WORK

Our future work in additional add the advanced security for access the website by adding the biometric authentication and one time password algorithm. The password is generating after the data is leakage which is send to the corresponding distributor mobile number or mail id. In this manner, the guilty user cannot access the distributor id. Hereafter, this type of adding some security system the data leakage must avoid the unauthorized party to secure industries and organization**.**

REFERENCES

1)Chandni Bhatt, Professor Richa Sharma (2014), *Data Leakage Detection***,** IJCSNS International Journal of Computer Science and information technology, Volume 5, No.2, .

2) Janga Ajay Kumar and K. Rajani Devi (June 2012),**"** *An Efficient and Robust Model for Data Leakage Detection System***"** Journal of Global Research in Computer Science Volume 3, No. 6, , ISSN: 2229-371X.

3) Nikhil Chaware, PrachiBapat, RitujaKad, ArchanaJadhav, Professor S.M.Sangve(Oct 13), **"***Data Leakage Detection***"** Journal of Information, Knowledge And Research In Computer Engineering, ISSN: 0975 – 6760| Volume – 02, Issue – 02| Page 534.

4) Rudragouda G Patil (2011), "*Development of Data leakage Detection Using Data Allocation Strategies***"** International Journal of Computer Applications in Engineering Sciences [Volume I, ISSUE II,], [ISSN: 2231-4946].

5) Anusha.Koneru, G. Siva NageswaraRao, J.VenkataRao (June 2011)**"** *Data Leakage Detection Using Encrypted Fake Objects***"** IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, .

6)PriyaWalunj, PriyaTadge, NavnathKondalkar, SatishMahamare (2015),**"***Identification of Data Leakage and Detecting Guilty Agents Using Data Watcher***",** International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 2, ISSN: 2277 128X.

7)KeerthiPagadala , Martha Sheshikala, D.RajeswaraRao (2013),**"** *Guilty Agent Detection by Using Fake Object Allocation***"** International Journal For Development Of Computer Science & Technology Issn-2320-

7884 (Online) Volume-1, Issue-V , ISSN-2320-7884.
8)RamjiShinde et al,"*Data Leakage Detection using Fake Objects for Suspected Users"* International Journal of Computer Science & Communication Networks, Volume 4(6),214-215 , ISSN:2249-5789.

9)Siyuan Ma; Department of Computer Science & Eng., Shanghai Jiao Tong Univ., Shanghai, China ; Zhushou Tang ; Qiuyu Xiao ; Jiafa Liu (2013),"Detecting GPS information leakage in Android applications" 2013 IEEE Global Communications Conference (GLOBECOM), Page(s): 826 – 831 ISSN : 1930-529X,2013.

10)ZhongXiu-yu ; School of Computer Science, Jiaying University, Meizhou, Guangdong, China (2010), " *A model of online attack detection for computer forensics*" International Conference on Computer Application and System Modeling (ICCASM 2010) (Volume:8), Page(s): V8-533 - V8-537 ISSN : 2161-9069, .