SECURE AND DETECT THE UNAUTHORIZED ACCESS OF EXPOSURE DATA

P. S. Kannan* & M. Rajakumar**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Associate Professor & Head, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

The data from investigate organizations, safety firms and government organizations demonstrate that the numbers of data leak instances have developed rapidly. Among different data leak cases, major causes of data loss are one of the human being mistakes. Present live solutions detect unintentional responsive data leaks caused by human being mistakes and to provide alerts intended for organization. In this system, there a privacy preserving data leak detection solution where a particular set of receptive data digests is used in discovery. Privacy-preserving data-leak detection representation intended for preventing inadvertent data leak in scheme traffic. Such a demonstration yields a powerful and delegatable data-leak detection framework. The cloud computing surroundings the cloud source can perform data leak detection as add on service to its customers. The assessment results show that the detection method can supports accurate detection through very miniature number of false alarms under various data leak scenarios. The benefit of this method is that it enables the data owner to safely hand over the detection operation without enlightening the sensitive data to the source.

Index Terms: Data Leak, Network Security, Privacy & Collection Intersection

1. Introduction:

Network protection consists of the policies adopted to prevent and monitor unauthorized access, misuse, alteration, or denial of a computer and network-accessible possessions. Network protection involves the approval of access to data in a system, which is proscribed by the network supervisor. Users choose or are assigned an ID and password or additional authenticate information that allows them contact to information and programs within their influence. System security covers a variety of computer networks, both communal and private, that are used in daily jobs; conducting transactions and communications among businesses, management agencies and individuals. Networks can be private, such as within a corporation, with others which might be open to communal access. Network security is involved in organizations, enterprises, and other categories of institutions. It does as its title give details: It secures the network, as well as protecting and supervision process being done. The most common and easy way of protecting a network resource is by assigning it a unique name and a corresponding password.

Detect and prevent information leaks requires a set of corresponding solutions, which may include information-leak detection, information confinement, stealthy malware detection and policy enforcement. Network information-leak detection (DLD) typically search for some occurrence of responsive information patterns and performs deep packet inspection (DPI). DPI is a technique to analyze payloads of TCP/IP packet for inspecting application layer information, e.g., HTTP header/content. Alerts are triggered and traffic passes a threshold when the amount of sensitive information found. There are two types of input sequences in information-leak detection model: sensitive information sequences and content sequences. Sensitive information contains the sensitive information that cannot be exposed to illegal parties, e.g., proprietary documents, customers' records. Sensitive information can also be partitioned to small sensitive information sequence. Content is the information to be inspected occurrences of sensitive information patterns. The detection need to divider the unique content stream into content segment.

In this system, the information-leak detection solution which can be deployed and outsourced in a semi honest detection environment. The fuzzy fingerprint technique is used enhances information privacy during information-leak detection operations. This approach is based on practical one-way computation on the sensitive information (classified documents, sensitive emails, SSN records, etc.). This enables the information owner to securely delegate the content check task to DLD source with no exposing the responsive information. By using the detection method, the DLD source, who is modeled as honest-but-curious adversary, and it only gain limited knowledge of sensitive information from either the release digests.

Using these techniques, an Internet service source (ISP) provides information-leak discovery as an add-on check for its clientele. The detection procedures of information owner compute a special set of fingerprints or digests starting the sensitive information. The DLD source computes fingerprints from network traffic and identifies potential leaks. To stop the DLD supplier from assembly exact knowledge about the sensitive information and the collection of potential leaks is composed of noises and real leaks.

The information owner who post-processes the potential leaks sent back by the DLD source and then determines whether there is any real information leak. Typical methods to stop data leak are under two types – host-based solutions and network-based solutions.

2. Related Works:

Cryptography-based multi-party calculation is not well-organized enough for practical data leak inspection in this setting. Propose, put into practice, and assess a new privacy-enhancing data-leak detection system that enables the data owner to securely delegate the traffic-inspection task to DLD providers without exposing the sensitive data. It is hard for a DLD source to learn the precise worth of sensitive data during the detection process. In our model, the data owner computes a particular set of digests or fingerprints as of the responsive data, and then discloses simply a small amount of digest information to the DLD provider.

These fingerprints have significant properties, which stop the supplier as of ahead information of the responsive data, while they enable accurate comparison and detection. The DLD provider performs deep packet inspection to identify whether these fingerprint patterns exist in the outbound traffic of data owner's organization or not. Do extensive experiments with real world datasets in a variety of data-leak scenarios to confirm the correctness and efficiency of future solutions. Aid is summarized as follows.

Explain privacy-preserving data-leak detection (DLD) model for stop inadvertent data leak in network traffic. Such a representation yields a powerful and delegatable data-leak detection framework. For example, in the cloud computing environment the cloud provider can perform data-leak discovery as an add-on service to its clients. Describe a quantitative privacy model needed for data-leak discovery as a service. Design, apply, and evaluate a new and efficient technique, fuzzy fingerprint, for realizing privacy-preserving data-leak detection. Fuzzy fingerprints are special digests of the responsive information that the data owner releases to the DLD provider. Explain the process in protocol that is run between the data owner and the DLD provider.

3. Proposed Work:

The system model in this project involves three parties: the cloud server, a group of users and a public verifier. There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. The data owner share the data into the cloud users, and the users should be access the data securely. The data should be transmitted from the data owner on securely through network. The unauthorized users can access the account that can be predicted in this method. If the unauthorized person tries to access the user account that can be predict and monitored on this method. And also identify the details about the user, IP address and details of the user. Thus the details are transferred to the authorized Person. The message can be transferred from source to the destination that time using the cryptography method. The source is encrypt the message using the public key of the receiver and then sends to the destination. The receiver can be decrypting the message using the private key. That time unauthorized Persian performs the illegal activities that can be predicted. The private key is not matched to the decryption process then identifies the user details, IP address. Thus the details are transferred to the sender side. The Privacy preserving data-leak detection (DLD) solution to solve the issue where a special set of sensitive data digests is used in detection. The advantage of our method is that it enables the data owner to safely delegate the detection operation to a semi honest provider without revealing the sensitive data to the provider.

Advantages:

- ✓ Using the technique of Perturbation data is made less sensitive for the agents to handle.
- ✓ Realistic but fake objects are injected to the distributed data set to identify the guilt agent.
- ✓ If two agents have same probability then the FIFO order is maintained to show the guilty agent.
- ✓ Possibility of full service with maintenance and SLA in overall service.
- ✓ Easier access to new software versions.

Modules:

- ✓ Data Allocation Module
- ✓ Optimization Module
- ✓ Secure transaction
- ✓ DLD on user side

Data Allocation Module: The main focus of our project is the data allocation problem as how can the distributor "intelligently" give data to agents in order to improve the chances of detecting a guilty agent. The problem of allocating the data of a database to the sites of a communication network is investigated. This problem deviates from the well-known file allocation problem in several aspects. First, the objects to be allocated are not known a priori; second, these objects are accessed by schedules that contain transmissions between objects to produce the result.

Optimization Module: The Optimization Module is the distributor's data allocation to agents has one constraint and one objective. The distributor's constraint is to satisfy agents' requests, by providing them with the number of objects they request or with all available objects that satisfy their conditions. His objective is to be able to detect an agent who leaks any portion of his data.

Secure Transaction: Each user is assigned to data owner from the Provider. Each user can freely get the cipher texts from the server. To decrypt a cipher text, each user may submit their secret keys issued by data owner together with its secret key to the server and ask it to generate decryption token for some cipher text. Upon receiving the decryption token, the user can decrypt the cipher text by using its secret key. The users those who are having matching keys as in the access policy defined in the cipher text can retrieve the entire data content. It aims to allow the users with eligible attributes to decrypt the entire data and access the data. However it cannot limit the users from accessing the data's which are not accessible to them. That is it cannot limit the data access control to the authorized used.

DLD on User Side: The user access the data from the service provider, decrypt and got the original data. The unauthorized person access the secure data from the service provider on the person account and miss use the account. If the account hack into the unauthorized person or another person enters into the account, the server sides read the current details about the user and ip address of the system if the authorized user receives the unsecured message and then change the account user name and password.

4. Experimental Analysis and Results:

Goal is to detect when the distributor's responsive information has been leaked by agents, and if possible to identify the agent that leaked the data. Perturbation is a extremely useful method where the data is customized and made "less sensitive" before being handed to agents. Expand unobtrusive techniques for detecting leakage of a set of objects or record in this section we develop a model for assessing the "guilt" of agents. Also present algorithms for distributing objects to agents, in a way that improves our chances of identifying a leaker. Finally, also consider the option of adding "fake" objects to the distributed set. Such objects do not correspond to real entities but appear realistic to the agents. In a sense, the fake objects acts as a type of watermark for the entire set, without modifying any individual members. If it turns out an agent was given one or more fake objects that were leaked, then the distributor can be more confident that agent was guilty.

Performance Evaluation:

To find the solution on this problem develop two models. First, when any employee of enterprise access sensitive data without the consent of owner in that case, we developed data watcher model to identifying data leaker in this point suppose data leaker will identify then no need to calculating the probability of agents that method gives near about 90 % of result. But suppose employee given data outside the enterprise for that devolved second model for assessing the "guilt" of agents. Guilt model are used to improve the probability of identifying guilty third parties. In this approach, the model for assessing the "guilt" of agents is developed. The option of adding "fake" objects to the distributed set are considered. Such objects do not correspond to real entities but appear practical to the agents. In a sense, the fake objects acts as a type of watermark for the entire set, without modifying any individual members. If it turns out an agent was given one or more fake objects that were leaked, then the distributor can be more con dent that agent was guilty.

Experimental Setup

Database Maintenance: Here the agent registration details are maintained and the sensitive data which are provided to agents are specified. The designing of the whole database is done.

Agent Maintenance: Registration: Here details of agents are registered and it collects the information about them like what are the sensitive data they want. History: Here the agent history is maintained like what all the details are given by distributor previously. It maintains entire details of the agent. To detect the guilty agents it checks the history and detects those agents who have fake details from the third party.

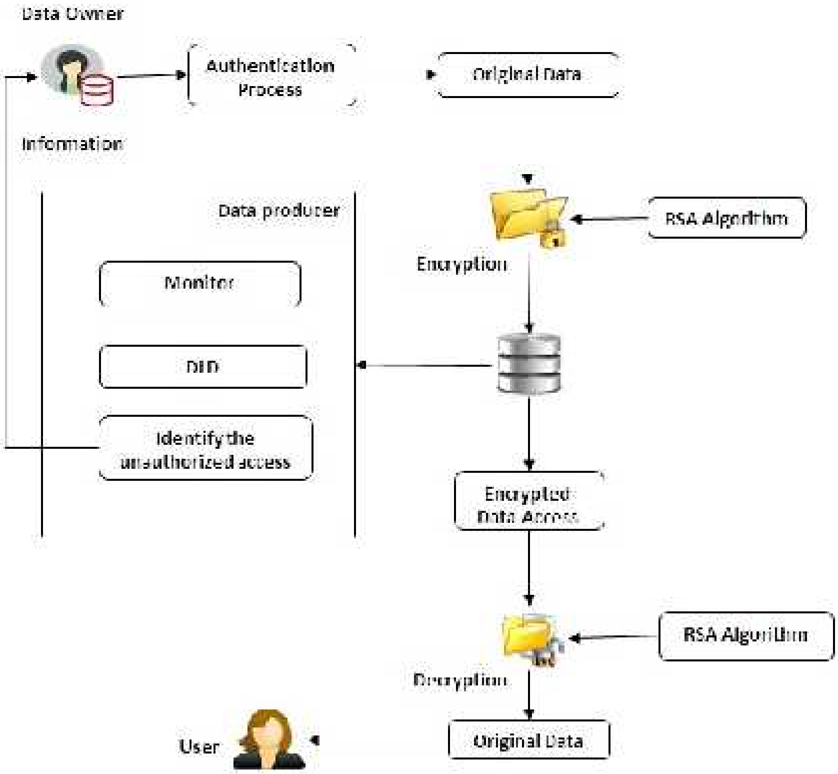

Figure 1: System Architecture

Detecting Guilty Agent: Suppose that after giving objects to agents, the distributor discovers that a set S has leaked. Since the agents U1....UN have some of the data, it is reasonable to suspect them leaking the data. For example, say one of the objects in S represents a customer X. Perhaps X is also a customer of some other company, and that company provided the data to the target. The goal is to estimate the likelihood that the leaked data came from the agents as opposed to other sources. If one of the S objects was only given to agent U1, while the other objects were given to all agents, suspect U1 more. It says an agent Ui is guilty and if it contributes one or more objects to the target.

5. Conclusion:

The privacy preserving detection method is used to secure sensitive data from the exposure. Using some special digests the disclosure of the sensitive data is kept to minimum during detection. The conduct extensive experiment to validate the correctness, privacy, and efficiency of our solutions.A novel privacy-preserving data-leak detection model and its fuzzy fingerprint realization. Using special digests, the exposure of the sensitive data isKept to a minimum during the detection. Conducted extensive experiments to validate the accuracy, privacy, and efficiency of our solutions.

6. Future Enhancement:

In future to implement the advanced security system based on encryption concept. The proposal of data security guide to the development of Cryptography.Cryptography is the science of maintenance data secure. Its encryption and decryption of data. Encryption is the process of change a plain text into cipher text and decryption is the process of receiving back the original data from the encrypted text. Cryptography, in adding together to providing confidentiality, also provides verification, Integrity and Non-repudiation. The crux of cryptography lies in the key concerned and the secrecy of the keys used to encrypt or decrypt. Another significant factor is the key strength, i.e. the size of the key so that it is not easy to perform a brute force on the plain and cipher text and get back the key. There have been a variety of cryptographic algorithms recommended.

7. References:

1. S. Ojala, J. Keinanen, J. Skytta, "Wearable authentication device for transparent login in nomadic applications environment," Proc. 2nd International Conference on Signals, Circuits and Systems (SCS 2008), pp. 1-6, 7-9 Nov. 2008.
2. T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, April 2007.
3. L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication System," Computer Safety, Reliability and Security, F. Ortmeier and P. Daniel (eds.), Lecture Notes in Comuter Science, Springer, vol. 7613, pp. 209-221, 2012.
4. S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc. 21st Annual Computer Security Applications Conference (ACSAC '05), pp. 441- 450, 2005. IEEE Computer Society, Washington, DC, USA.
5. U. Uludag, and A. K. Jain, "Attacks on Biometric Systems: a Case Study in Fingerprints," Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, pp. 622-633, 2004.