International Journal of Pure and Applied Mathematics
Volume 119 No. 10 2018, 393-398
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Data Leakage Detection during Transmission

[1]P.V. Kumaraguru and [2]V.J. Chakravarthy
[1]P.G. Department of Computer Applications,
Guru Nanak College, Velachery, Chennai.
pvkumaraguru@gmail.com
[2]P.G. Department of Computer Applications,
Guru Nanak College, Velachery, Chennai.
chakku_vjc@yahoo.co.in

Abstract

In the present world everything worked using network including data entry, digital economy and leaves cyberspace at record rates. An usual enterprises receive and send millions of messages, download in emails and also transfer more than thousand of files over several channels on a everyday basis. In organization or enterprises, the main dangerous threat facing in day today life is leakage in confidential data. Leakage of data is said to be unintentional distribution of data which is private and sensitive data to an illegitimate entity. Information's based on patient data, financial data, personal banking data and credit card information like sensitive data of individual persons and business information were shared through network may lead to chance of data vulnerability and data leakage during exchanging of information. So to avoid these kinds of difficulties, the data leakage detection method has been introduced and proposed. The study of paper includes brief ideas and methodology based on leakage detection of data during transmission.

Key Words: Detection, transmission of data, data leakage.

1. Introduction

The information value is outlandish, however it should not be changed or leaked. However, there is numerous system designed by using various encryption algorithm for data security. In enterprises, leakage of data is a vast challenge. Therefore it creates the numerous ethical issues in the organizations of the working environment. It is a huge problem of reliability of the client in these system and also firm track the data leaker by any system administrator among the system users[1]. The unauthorized transfer of sensitive and private data to third party is said to be a data leakage, the unauthorized recipient receive the data from an entity or person. In the present world financial and private data need to be shared among different stake holders such as business partner, employee and share holding customer by the distributor. The detection of data leakage is done because of authoritative agent who can access the data easily [2]. Trusted agent such as mediator where the few confidential information was found in unapproved that was get leaked. The distributor had done the assessment based on data leaked which came from the more than one agent as contrasting to have separately gathered by other resource. The proposed design of data allocation over the agent should advance the probability of identifying leakages [3].

2. Literature Review

Today life every organization and company require data security from the cyber crime where data is an essential components to all company, so the annihilation of data and data loss became a common issue. In the IT Organization, every moment large amount of information is transferred to many third parties and several people. However while data transmission there are several probability in vulnerability of data and data leakage during the transmission of information. In order to overcome these difficulties securely through the study of leakage of data detection based on web and some prevention system is required. According to this survey, the methodology and technique is for identifying the data leakage [4]. Data security is a significant for most of the business users and also for home computer users.

Private and confidential information are personal information, financial information, banking details like bank account, credit card information which it is tough to change and may also highly dangerous due to these secure data fall into wrong hand. Data loss due to natural disaster like flood or firing is not an issue but Data loss creates much greater consequences in which the hacker or malware infection from wrong hand. The hetrogeneous data leakage detection is progressed in the prominent IT security vendor with developed product lines.

The widely ordnance of indulgent method such as firewall, encryption, identity management, access control, etc has already included to offer prevention against various facets of data leakage based on threat [5]. In this research, usage of water marking is for data leakage detection where the model can be recognized as the

result for implementation. For example embedding the unique code on each distributed copy, uncertainly the copy is found in the hand of illegal person, and for that leaker can be identified [6].

3. Methodology to Provide Data Leakage Detection

Data handling policies for Creating and imposing organization-broad is based on the industry regulations and also specific requirements organization's which are important to standardize all features of handling particular data in an association. These data handling policies proclaim strict rules for control these types of data, such as discarding or archiving unneeded subjective information and creating access control mechanisms to authorize access to such data by authorized staffs only.

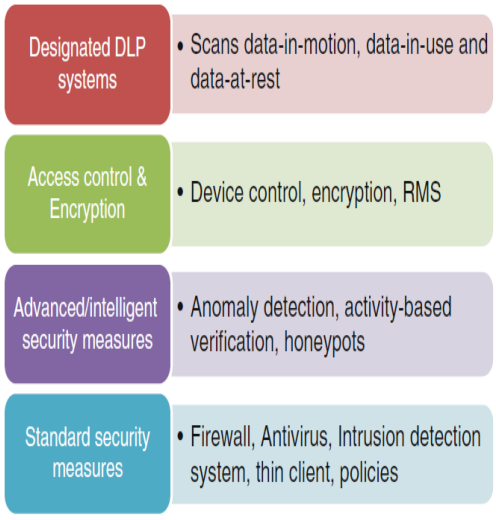

Figure I: Classifications of Technological Approaches used to Provide Data Leakage Recognition and Prevention

The data handling policy created should be supplemented by suitable training that notifies employees of the instructions and a requirement that employees sign binding reports concerning their responsibilities and their commitment to work affording to the policy.

Advanced or Intelligent Security Processes

To detect unauthorized access of data it includes the algorithms such as machine learning and temporal reasoning algorithms (i.e., databases or information recovery methods), verification based on activity (e.g., based on keystrokes and mouse patterns), detection of unusual mail exchange forms, and put on the honey pot idea for detecting malicious insiders.

Device Control, Access Control, and Encryption

To protect huge amounts of private documents these are the modest methods that can be taken against malicious outsider and insider attacks. These are used to prevent the access by an unauthorized user.

Designated DLP Solutions

It is suggested to identify and prevent challenges in copying or sending sensitive information, intentionally or unintentionally, without endorsement, generally by personnel who can able to certify the sensitive information access. A key ability of such results is an ability to categorize the content as sensitive [7].

4. Data Leakage Detection Modules

Module Based on Data Allocation

In this data allocation module, there is a chance of sensing the agents which leaks the data. These agents identify the secret key information by email. The main aim of data allocation is the agent from the distributor, how to get the data in director to rising the risks in identifying a guilty agent. Authorized users receive the files from the administrator. Account details can be edited by the users.

Fake Object Module

The creation and addition of fake objects along with the original data by the distributor and send the files to the agents. Fake object is an object which is used to improve the chance of identifying the agent that who has leaked the data by the distributor. The distributor probably is by adding fake object into the data distribution to improve the efficiency and effluent of guilty agent detection. The distributor by adding fake object to trace the record of duplicate agent in mailing list of leak data. The invalid secret key is send to the agent by the distributor download the data, the file opened is a duplicate file, and that the fake information also sends to the mail. Ex: The fake information will be demonstrated [5].

Optimization Module

In this Optimization Module, one constraint and one objective is allocated to the agents by the distributors. The request of the distributor is to be fulfilled by the agent constraints. Their conditions are satisfied with all the obtainable objects which they demand with the numbered objects or by providing them. This is the possible way to analyze an agent who can leaks the data at any part of his information. The user can accomplished for security purpose to unlock and lock the files.

Data Distributor Module

In the data distributor module, the data distributor can set of purportedly the sensitive data which is given to third parties. In that lot of leaked and available data from the unauthorized location like web abd some one’s laptop. The files

leaked are proposed from more than one or a single agents in which distributor must consider the chance to have been contrasting the individually assembled by other resources. The fake and leaking of user's details is also can be finding out by the administrator.

Agent Guilt Module

If Ui is the guilty agent ,then the destination have one or more objects is gives from Ui. The S is leaked set which it is represented by Gi | S is given as the event of guilty agent Ui . The steps to evaluate the probability of agent Gi which is guilty that given to evidence S. It is denoted by Pr (Gi | S). In order to calculate the probability of guilty to calculate the value of probability in S which can also be estimated by the target [8].

5. Conclusion

This paper exposes the data leaks involve in issue of sensitive information to the third party which is unapproved user intentionally. Leakage is transmission of information which is unauthorized within an organization to the external destination, while transmission or distribution of data. To overcome this kind of problems, data security is essential to an organization. Therefore by the usage of this detection model, tracing system and also the security system get improved. This model is very helpful in several industries in which the data is distributed via various channel and it is shared with authorized agents. Now most of the industries and various organizations have depend on on leakage of data detection model for data security.

Reference

[1] Grinal Tuscano, Humairah Kotadiya, Vikrant Bhat, Rollan Fernandes, Amod Panchal, A Survey on Data Leakage Detection 5 (4) (2015), 153-158.

[2] Richa Desai, Megh Jagad, Abhijit Patil, Data Leakage Detection Using Data Allocation Strategies 4 (11) (2015).

[3] Jyoti Nevase (Raut), Punam Chougale, Sneha Shewale, Bhosale, Data Leakage Detection 3 (5) (2017).

[4] Senha Sewale, Jyoti Navse, Punam Chougale D.M., Bhosale A., Study on Determining Data Leakage Detection 2 (12) (2016).

[5] Sandip A.K., Kulkarni S.V., Data Leakage Detection 1 (9) (2012).

[6] Neha S.B., Keole R.R., An Overview of Data Protection by Data Leakage Detection 3 (1) (2016).

[7] Shabtai A., Elovici Y., Rokach L., A Survey of Data Leakage Detection and Prevention Solution, 2012.

[8] Rudragouda G.P., Development of Data Leakage Detection using Data Allocation Strategies 1 (2) (2011).