ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Review on Security on Data Using Encryption and Steganography

Bondare Dipak, Sayyed Tabish, Shetiya Siddhi

B.E. Student, Department of Computer Engineering, V.A.C.O.E. Ahmednagar, Maharashtra, India

ABSTRACT: Researchers have proposed several mechanisms to secure data from unauthorized use but there is very less work in the field of detecting and managing an authorized or trustworthy agent that has caused a data leak to some third party unknowingly. In this paper, we implement methods aimed at improving the odds of detecting such leakages when a distributer's sensitive data has been leaked by trustworthy agents and also to possibly identify the agent(s) that leaked the data. We also implement some data allocation strategies that can improve the probability of identifying leakages and can also be used to assess the likelihood of a leak at a particular agent assuming the fact that the data was not simply guessed by the third party where the leaked data set has been found. We also propose new allocation strategies that work on the basis of No-Wait model, i.e. agent does not need to wait for other agents' allocation and it is different from already proposed model that makes an agent wait for others. These methods do not rely on the alterations of the distributed data, but rather focus on minimizing the overlapping of the allocated data items to various agents, thus facilitating an exact determination of the guilty agent in a particular data leakage scenario.

KEYWORDS: - Allocation Strategies, Data privacy, Data Leakage, Detection and Prevention, Guilt model.

I. INTRODUCTION

Data distributor has given sensitive data to a set of supposedly trusted agents. Sometimes data is leaked and found in unauthorized place e.g., on the web or on somebody's laptop. For example, a hospital may give patient records to researchers who will devise new treatments. Similarly, a company may have partnerships with other companies that require sharing customer data. Another enterprise may outsource its data processing, so data might be given to various other companies. The owner of the data are called as distributors and the trusted third parties are called as agents. Data leakage happens every day when confidential business information such as customer or patient data, company secrets, budget information etc. are leaked out. When these information are leaked out, then the companies are at serious risk. Most probably data are being leaked from agent's side. So, company have to very careful while distributing such a data to an agents. The Goal of Our project is to analyze "how the distributer can allocate the confidential data to the Agents so that the leakage of data would be minimized to a Greater Extent by finding a guilty agent"

II. RELATED WORK /SURVEY

Early work in the area of data leakage detection resulted in the idea of using watermarks within sensitive digital information. Here, a uniquely identifying text or image is embedded within each copy that is distributed to authorized agents. When leakage occurred, then this unique code would help identify the party that was responsible for the leak. The problem with this approach was that even though this is an easy solution, it still involves a certain modification of the original data information set. Also, it was observed that such watermarks could be tampered with to sufficiently distort the uniquely identifying code or sometimes completely destroyed if the data recipient is malicious. In their paper, they proposed the main premises on which much work in this area has been based. They propose several data allocation strategies (across the agents) that improve the probability of identifying leakages. The chief contribution here was that the proposed techniques were not based on altering the distributed data in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

any way, but allocating the data intelligently so as to identify the guilty party. Also, in the case of data leakage from trusted agents, the distributor must evaluate the odds that the leaked records came from one or more agents

III. PROPOSED SYSTEM

Goal is to detect when the distributor's sensitive data has been leaked by agents, and if possible to identify the agent that leaked the data. Perturbation is a very useful technique where the data is modified and made "less sensitive" before being handed to agents. We develop a model for assessing the "guilt" of agents. We also present algorithms for distributing objects to agents, in a way that improves our chances of identifying a leaker. Finally, we 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.

a. Distributor

What Distributor will share?

I. Media File
II. CSV File
III. HTML page

Sharing Media files to Agents

i. Distributor will encrypt secure data using RSA algorithm and then hide it into file using random bit Steganography
ii. When steganography successfully done he will share these files to set of agents to make these files to give to the end user
iii. To make these files available he will upload these files to the server

Sharing content/data to the Agents

a. Finding which type of data have to be share
b. Adding agents details as a fake object into the data/content

Detecting The Guilty Agent:

Whenever files from distributor makes available to the agent he can download these files.In backend when he downloads these file the signature of agent will be added to the file using RSA and steganography.Whenever distributor finds the file on unauthorized user's site he can download and do reverse steganography from which he will get the encrypted data by decrypting it he will get his signature as well as the agent's signature.From which guilty agent will be detected.Or by finding agents details from the data which has been added as a fake object/record Optimization.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 the data or lock the file so that it cannot be distributed or leaked

IV.ALGORITHM

RSA ALGORITHM

Before hiding data into the file we encrypt data using RSA algorithm.

To Encrypt data using RSA algorithm :

Cipher = ((data)d mod n)

Where

i. Cipher = encrypted text
ii. data = text to encrypt
iii. d = public key to encrypt the data
iv. n = length of key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

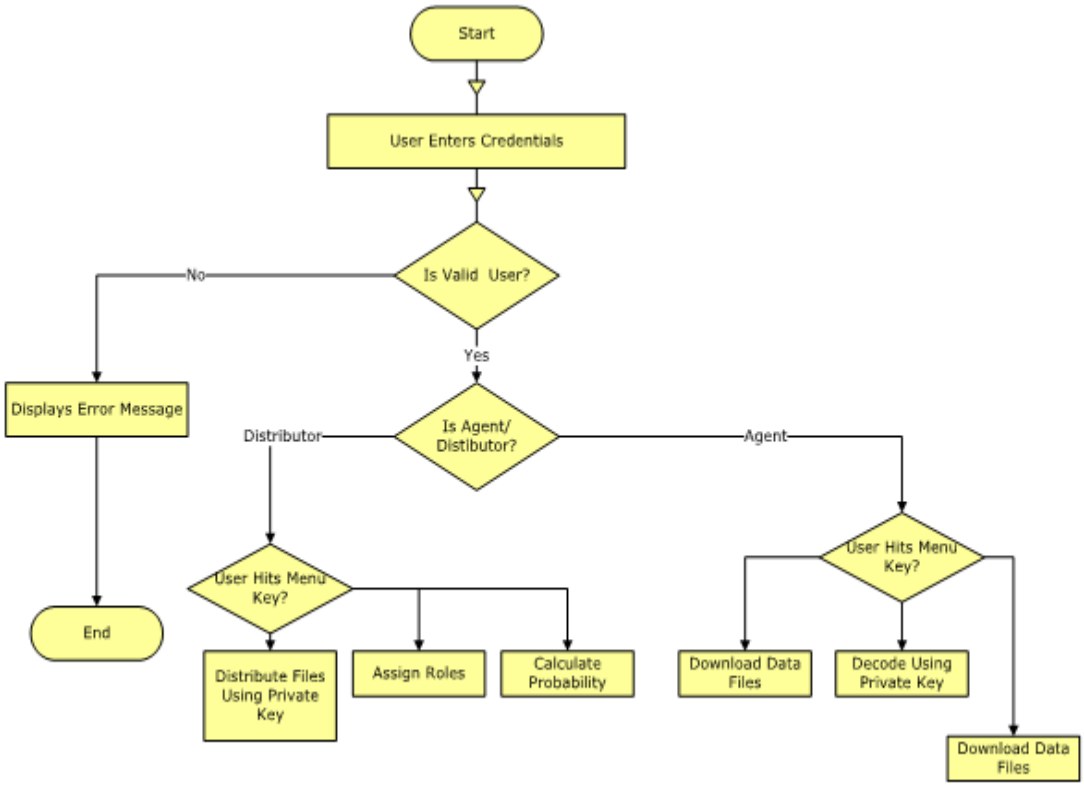
To Decrypt data using RSA algorithm :

data = ((cipher)e mod n)

Where

i. Cipher = encrypted text
ii. data = plain text
iii. d = private key to decrypt the data
iv. n = length of key

V.WORK FLOW DIAGRAM



VI. GOALS AND OBJECTIVES

To detect the agent who leaked the confidential data and send alert message to the distributor.The objectives of the "Data Leakage Detection" are as follows:

i. Detection of guilty agent
ii. Send message or email to the distributor with identification of guilty agent
iii. Send alert message to the guilty agent
iv. Take legal action on agent when he/she break rule after the alert message

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

VII. CONCLUSION AND FUTURE SCOPE

Thus we have designed the overall architecture of the project and we have learnt the RSA Algorithm. We have used the encryption and Decryption of data. We have studied the steganography and reversed-bit Steganography, we also learnt swings in java.

Future Scope

It provides higher security as only admin knows how to find the guilty agent and we can detect the data leaked. as administrator has the rights of both distributor, agent and admin has its own rights also. In future it is beneficial for preventing data leak or data loss.

ACKNOWLEDGEMENT

The author would like to thank the Questions and suggestions the Anonymous Reviewers that helped to improve this document. It gives us great pleasure in presenting the preliminary project report on “DATA LEAKAGE DETECTION”

REFERENCES

[1]Agrawal and J. Kiernan, “Watermarking Relational Databases,” Proc. 28th Int’l Conf. Very Large Data Bases (VLDB ’02),
[2]P. Papadimitriou and H. Garcia-Molina, “Data Leakage Detection,” technical report, Stanford Univ., 2008.
[3] N. P. Jagtap, S. J. Patil, A. K. Bhavsar, “Implementation of data watcher in data leakage detection system”, International Journal of Computer & Technology Volume 3,No. 1, Aug, 2012.
[4]Ankit Agarwal, Mayur Gaikwad, Kapil Garg, Vahid Inamdar, “Robust Data leakage and Email Filtering System”, International Conference on Computing, Electronics and Electrical Technologies, 2012.