International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

Preventing Information Leakage in Distributive Strategies by using One Time Password base Authentication

Miss. Priyanka P.Tikhe1
Department of Computer Science & Engineering RTMNU University
priyanka17tikhe@gmail.com
Miss. Pooja D. Bhoware2
Department of Computer Science & EngineeringRTMNU University
pooja.bhowre15@gmail.com
Mr. Naveen D. Shende3
Department of Computer Science & Engineering RTMNU University
naveenshende@gmail.com

Abstract —

Nowadays privacy and security of the data plays an important role in every field or business. Every company or organization wants their confidential data private. Some distributer or a -BPO company has given sensitive data to a set of supposedly trusted companies or a set of users. The data is distributed to third parties is found in a public/private domain. Finding the guilty party is a nontrivial task to distributor. Traditionally data leakage is handled by water marking technique which requires modification of data. If the watermarked copy is found at some unauthorized site then distributor can claim his ownership. In this project, we implement a prevention technique by providing security to the file so that data will be more secured before handling by user. Also we are introducing the concept of One Time Password (OTP) for user authentication. Here we are sending files to the user in encrypted form using encryption algorithm so that files will be more secured. Data allocation strategies are used to improve the probability of identifying guilty agents and analyze it by inserting the fake objects with original documents. Designed system where provide security to the files that it will be kept secured.

Keywords—Data Security; OTP; Prevention; Detection; Fake Object

I. Introduction

Nowadays sharing information or data over network has become a very common and important practice. The data which is being shared over network should be in an encrypted form for the security purpose since the data which is being shared may be confidential or highly sensitive.

In the course of doing business, sometimes sensitive data must be handed over to supposedly trusted third parties. 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 must be given to various other companies. We call the owner of the data the distributor and the supposedly trusted third parties the Users. Our goal is to prevent when the distributor's sensitive data has been handover to users, and if possible to identify the Users that leaked the data. We consider applications where the

original sensitive data cannot be perturbed. Perturbation is a very useful technique where the data is modified and made "less sensitive" before being handed to users. For example, one can add random noise to certain attributes, or one can replace exact values by ranges. However, in some cases it is important not to alter the original distributor's data. For example, if an outsourcer is doing our payroll, he must have the exact salary and customer identification numbers. If medical researchers will be treating patients (as opposed to simply computing statistics) they may need accurate data for the patients. Traditionally, leakage detection is handled by watermarking, e.g., a unique code is embedded in each distributed copy. If that copy is later discovered in the hands of an unauthorized party, the leaker can be identified. Watermarks can be very useful in some cases, but again, involve some modification of the original data. Furthermore, watermarks can sometimes be destroyed if the data recipient is malicious [1].

II. Problem statement

To design a network based application which shall be able to prevent information over the network and provide protection to it by using Encryption algorithm and for security purpose we are providing verification process by using one time password (OTP) concept.

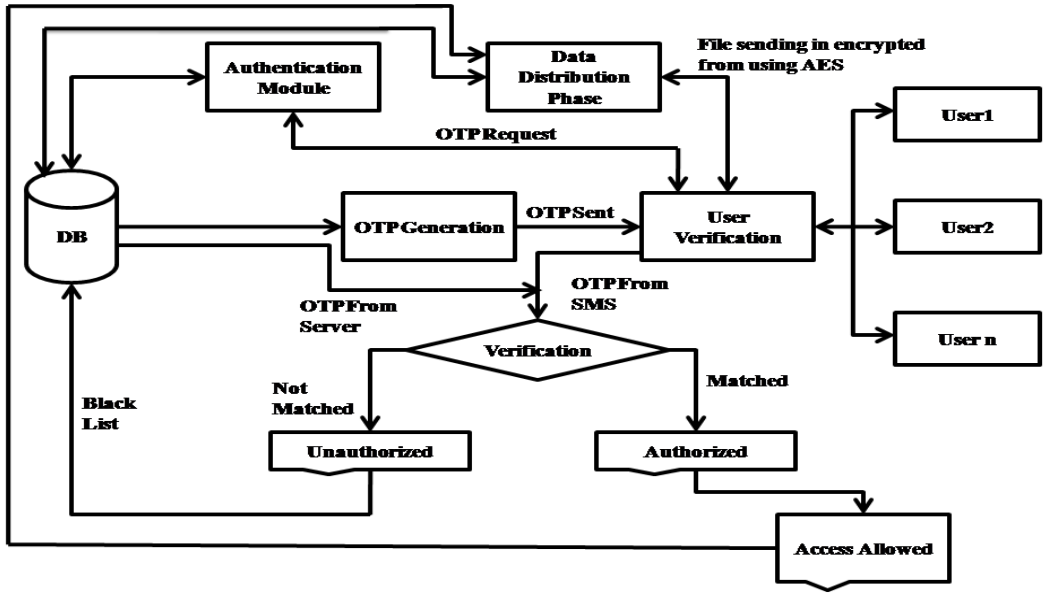
Objective:

- To protect data from leakage.
- To give security for the important data and files.
- Files or data can be access only by organization member.
- To identify the Users that leaked the data.
- Provide the web base solution to prevent the data leakage.

Overview:

Data leakage is the big challenge in front of the industries & different institutes. Though there are number of systems designed for the data security by using different encryption algorithms, there is a big issue of the integrity of the users of those systems. It is very hard for any system administrator to trace out the data leaker among the system users. It creates a lot many ethical issues in the working environment of the office. Traditionally, Data leakage is handled by watermarking, e.g., a unique code is embedded in each distributed copy. If that copy is later discovered in the hands of an unauthorized party, the leaker can be identified. Watermarks can be very useful in some cases, but again, involve some modification of the original data. In this project we study unobtrusive techniques for detecting leakage of a set of objects or records. Specifically, we study the following scenario: After giving a set of objects to users the distributor discovers some of those same objects in an unauthorized place. (For example, the data may be found on a web site, or may be obtained through a legal discovery process.) At this point the distributor can assess the likelihood that the leaked data came from one or more users opposed to having been independently gathered by other means. If the distributor sees "enough evidence" that a leaked data, he may stop doing business with him, or may initiate legal proceedings. In this system if user or Users want to access the file then the user must be registered user for OTP .In this Project we develop a model for assessing the "guilt" of Users. We also present algorithms for distributing objects to Users, 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 Users. In a sense, the fake objects acts as a type of water mark for the entire set, without modifying any individual members. If it turns out a User was given one or more fake objects that get leaked, then the distributor can be more confident that Users was guilty.

III Implementation method



Modules:

A. Data Distributor Module

A data distributor has given sensitive data to a set of supposedly trusted Users (third parties). Some of the data is leaked and found in an unauthorized place (e.g., on the web or somebody's laptop). The distributor must assess the likelihood that the leaked data came from one or more Users, as opposed to having been independently gathered by other means Admin can able to view the which file is leaking and fake user's details also.

B. OTP Generation Module

In verification process we are going to use the concept of one time password(OTP).For OTP ,the user or Users must be registered for authorization that the Users is from particular organization so that OTP can be send ,if the user is unauthorized then access will denied.

Advantages of OTP:

- Cannot be reused.
- Avoids expensive Hardware tokens.
- Can be time-limited.
- Can be used over untrusted communication paths.
- Multiple delivery mechanisms.

C. User authentication

In this module we check the user by his valid credential .In which user will enter their user ID and password .It will verify through the server database .If that login information enter by the user is valid then and then only the system will provide the access to the user at the same time OTP request will send to the server.

IV. Conclusion

The application development is not completed yet but once it would be finished it would serve to prevent data leakage. Our model is relatively simple. We propose a web base solution which will prevent the data leakage over the network using the OTP verification. Also, we are adding the fake object to the original file for data leakage detection purpose. It is a network based application which shall be able to prevent information over the network and provide protection to it by using Encryption algorithm and for security purpose. We are providing verification process by using one time password (OTP) concept.

REFERENCES:

[1] Panagiotis Papadimitriou," Data Leakage Detection," ppapadim@stanford.edu, Hector@cs.stanford.edu January 10, 2009

[2] Miss s.w.Ahmad," Data Leakage Detection And Data Prevention Using Algorithm", Dept of computer sc. & engg. P.r.m.i.t. & r, badnera

[3] Archana Vaidya, Prakash Lahange, Kiran More, Shefali Kachroo & Nivedita Pandey,"Data Leakage Detection,"Department of Computer Engineering, S.V.I.T., Nashik, M.H., India

[4] International Journal of Advances in Engineering & Technology, March 2012.©IJAET ISSN: 2231-1963316 Vol. 3, Issue 1, pp. 315-321

[5] William J. Blanke, "Data Loss Prevention Using Ephemeral Key", Symantec Corporation, 2011.

[6] International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012, Copyright to IJARCCE www.ijarcce.com 6686].