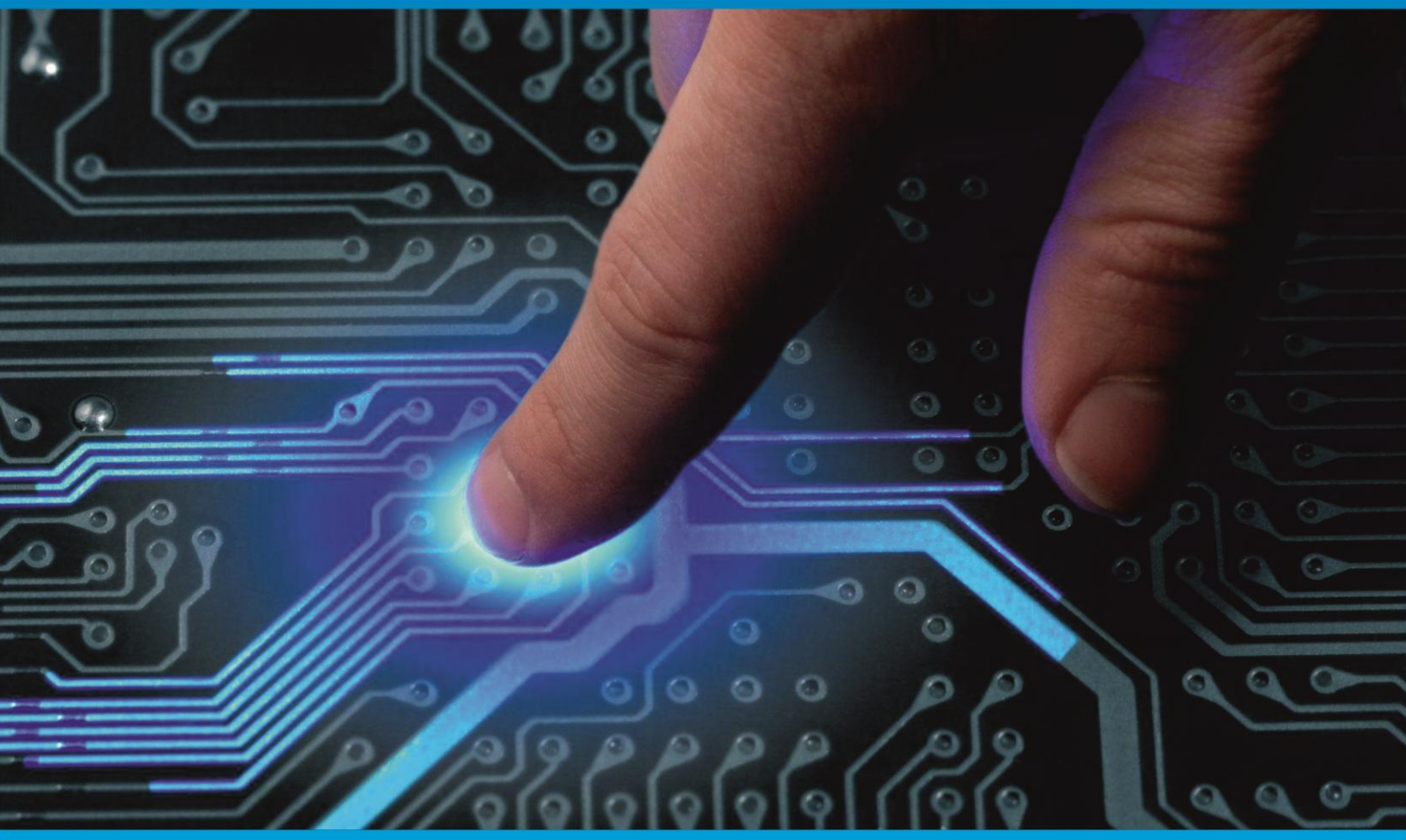
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905193 |

Cloud Based Data Dissemination Diagnosis and Interception

Mrs Rohini B. Gurav[1], Priya A. Kunwar[2], Vaibhavi R. Pawar[3], Parinita R. Waghmare[4]

Lecturer, Department of IT, AISSMS's Polytechnic, Pune, Maharashtra, India[1]

Student, Department of IT, AISSMS's Polytechnic, Pune, Maharashtra, India[2]

Student, Department of IT, AISSMS's Polytechnic, Pune, Maharashtra, India[3]

Student, Department of IT, AISSMS's Polytechnic, Pune, Maharashtra, India[4]

ABSTRACT: Today, many organizations do business, to another level. They do business through the various actors and institutions. Level up with the business community for storing and transmitting information from one place to another, to grow, and so, in the middle of, any user can leak information. Our main task is to detect the fault of the agent, which gave way to the leak of the confidentiality of your data. Information leakage can be described as a non-public possession of information in the environment of the server in the realm. This paper describes a model for the allocation of resources toward the provider, and the chosen one the least common agricultural policy, the distribution of the documents in the plan, such as a set of records for each customer, which can be very likely to discover the sources of the leaks. The confidentiality of the information of the organizations internal policies relating to the information economy, the information on the individual credit card, and information related to the organization of such confidential information may be leaked by an attacker. Data leak detection as models, the use of false objects, which are stored in the server database. Wrong object, it identifies the user who gave it leaked out of its path. Each user can have a chance of escaping this file to a probability, which is known as the sin of probability. The user of the probability of a leaked file is known as the sin of probability. Many of the data leak detection as a pattern of focus upon false objects, among other things, with a database of the detection system.

KEYWORDS: Data upload, the upload of the data, unauthorized access protection, data leak, aggressive, access to the database role.

I. INTRODUCTION

Many companies are now going from one stage to the next. They operate their business with the help of a variety of actors and organizations. As the business layer grows, so does the collection and transfer of data from one place to another, as it is possible for any user to leak the information. Our main goal is to find out who was responsible for the leak of confidential information. The unofficial moving data to the outside server, the kingdom is well-known for leaking the information. These items define the models, and the allocation of resources in order to counter the leak, and then select a lowest-common agricultural policy, the distribution of the document is the plan from a variety of customer database, which will make it very likely that, to identify the sources of the leak. The internal regulations of the company details of the money to the details of individual credit card, and in this structure is related to that of the confidential information that may come out of a circle. Information leakage is a big problem for a lot of different organizations. Data leak detection, the models tend to use a "fake objects", which are stored in the server database. Fake objects that will help you to determine the identity of the person who leaked them to the file. For all of the consumers, there is a chance that the file has an information leak, which is known as the sin of probability. Probably, but comes to the number of users who have a chance of leakage to the file. Many of the details to detect the presence of a leakage in the pattern is crucial in order to allow the false data, the effective databases in order to identify the leak.

In a bad business scenario, data leakage is a major problem, as a critical organizational data needs to be protected from access by unauthorized persons. The Information leakage may be defined as the intentional or unintentional disclosure of personal or critical organizational data to unauthorised persons. It's very important that the rules of the game or of the personal data, the abuse of any unauthorized use. Critical or private data, containing information about the reproduction of intellectual property rights, patent, functional, informational, and so on. Many of the organizations or government agencies to have a private organisation, they will present the information from outside the organization. It is, therefore, difficult to determine who is responsible for it, or the leaking of information. In the proposed work, our goal is to discover, to blame, or to put the blame on the user, as the organizational details have been leaked by an agent. In this proposal, the use of models, in order to ensure the security of the analysis and design of secure computing systems. According to the report, a sophisticated hacking attacks have occurred frequently, for some time. The Hacker's

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905193 |

attacks in the past, leading to the leakage of private information, however, over the past few years, hackers target businesses, organizations, government agencies, and organisations. This type of attack is called APT (Advanced Persistent Threat). APT, is a focus on specific systems, and analyse the vulnerabilities of the system for a long period of time. Therefore, it is very difficult to prevent and detect APT than traditional attacks, and may lead to a system corruption. the detection and prevention systems in place for the protection of

II. RELATED WORK

The distributor distributes the information to the registrar of the constraints and objectives. The limitation is that the agent must be in a file in order to complete the request. The distributor will maintain the tables and queries for the user. The lens is able to detect any leaks. The distributor selects the smallest of their way to send their files to the user, such as this file requires the. The model uses the minimum requirement in order to start a file and run it as a client to the user. Let's say a file on your computer is reporting a source to a destination (B), and among them, only two of the intermediates, that is, X and Y, if the file is leakage in the operation, the probability of the file, the leakage is (½). The source of the leaked document can be X or Y, but we have to use the method, if it has the same origin, and destination of the file transfer match, or do Not, there may be an intermediary figures between them, (n1, n2,..., nn). When a file is run through a process, an operation, then the probability that there will be (1/n), is there anything else that is difficult to find. Thus, the minimum of matches to be an effective way to find the perpetrators of the user [1].

The fake items are made by the distributor. The allocator add some of the fake objects to the actual data, in order to improve the effectiveness and efficiency of the detection of the source of the leak. The item is not genuine. It's just that will be generated during the operation, in order to track down the agent of the sin, for which you need in order to leak the information. Fake objects that were created in this way, the agent is not able to distinguish between the false objects of the real-world entity. The false labels are usually used to make use of the actual data, in order to track and control their own data, for example, the X, the company is selling an item on a Company Y. Company X's add some of the fake software, as well as to the company, the address of the Company, the Y, the misuse of the data in order to sell, remember, your data will automatically receive a copy of the company's problems in the notes, so that X can be easy to detect the misuse of the data. False, the given F= {f1, f2...,fn} of [2].

This is one of the works of S. N. holambe, [3] the distributors agents, there is an example with an explicit algorithm. Examples of the algorithm depends on a false object, according to the data source, in order to increase the probability of detecting an offence, the only difference is that the user is guilty person is found, and the first to accept the false object is delicious, but at the express request of wrong items, don't see it, it all depends on the agent's request. The vendor has the option to add multiple static wrong items, [3].

If the database is damaged or corrupted, there is a high chance of losing of information. That way, you can recover data from a corrupted file on your computer, use appropriate software tools. If you are working, electrical, appliances, laptops, COMPUTERS, etc., suddenly, turn off the power supply during the operation, there is a maximum chance of losing your confidential data. So, to avoid this problem is to continually maintain your work [4].

III. PROPOSED ALGORITHM

A. *Design Considerations:*

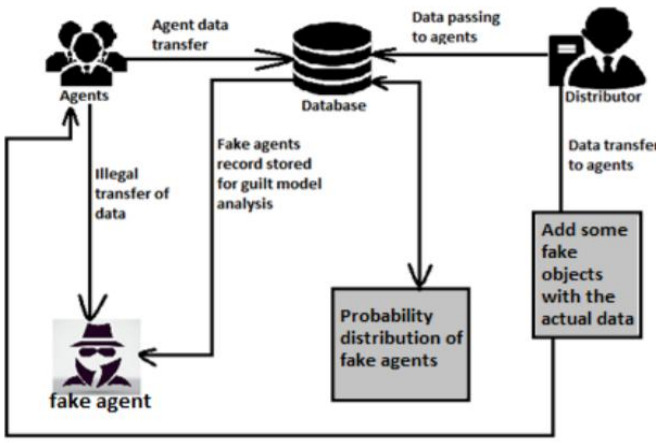


Fig 1. proposed system design

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905193 |

B. *Description of the Proposed Algorithm:*

This is a proposal of the system being studied and the methods used in order to detect the leakage of a set of objects or records. In particular, we study in this experience, in the following scenario: after the sending of a data set, the distribution of the agents to discover some of the data in an external, or improper site. For example, the information can be found on the web site, or obtained through a variety of legislative procedures. At this point, the distributor can assess the likelihood of information leakage, which occurred in the order of one or more agents, as opposed to what they have independently collected and in other ways as well. In the proposed system, we are getting ready for a system that defines the ' sin ' of the goals. We present algorithms for distributing objects among the different stakeholders in such a way as to increase the chances of detecting a leak of information. Finally, we are planning to add a “fake” object to the distributed data collection of the information provided by the distributor. Such objects do not correspond to real entities, but they seem to be in a real-time software agent, for this, we have to make a fake item. In a sense, the fake objects are a type of activity, such as a watermark, so that the number does not change an individual agent. If it turns out to be agent of the outside, as to one or more of wrong items, are leaking out, is a distributor, which the system can be confident that agent was guilty of sin. This is a proposal for a system in which information is delicious and can be traced back, with a great amount of evidence. This system is also a single archive of cost-cutting program that has its own file format. At the same time as they cut down the file of an employee in our organization, it will ask for administrator permission, if the administrator grants permission for the hair of the employee will have to download it. A login page is displayed to each user, both as an agent and a distributor. When a user logs in under his credentials (such as username and password), they can be identified as a Distributor or an Agent. As soon as the user is detected, the corresponding JSP page is displayed, in which he can transfer the files, the agent and track down the file-sharing between agents. To send files from the distributor to the agents, some of the incorrect item, the file will be sent to the agent. If an agent is sending the same file to another agent, it is determined, as has been said, that the obligation of the Distributor to determine what that is, it is the obligation of the agents under the supervision of the agency. The contents of this file will be removed, with the exception of the hidden items, if any, the agent will send the file to a different agent.

IV. PSEUDO CODE

Step 1: The distributor logins into the system.
Step 2: The distributor uploads the Data [example. text files] into the Database.
Step 3: Agent asks for the particular file or distributor uploads all file for agents accordingly along with private key after Login into the system.
Step 4: The distributor sends that requested file to the requested agents who add some fake objects.
Step 5: Agents will download the files according to his needs [Sample requests or explicit request].
Step 6: If any agents leak the data to the third party [Fake Agents] the distributor will check for the leaked data and will find the file which has been leaked.
Algorithm Design
SQL Injection and prevention algorithm for Database Security
Input: Query=User Generated Query, SPL[ ]=Static Pattern List with m AnomalyPattern
Step 1: Procedure SPMA(Query, SPL[ ])
Step 2: For j = 0 to m do
Step 3: If (AC (Query, String.Length(Query), SPL[j][0]) = =0)then
Step 4: Calc anomaly score
Step 5: If ( ) Score Value Anomaly = Threshold
Step 6: then
Step 7: Return Alarm.. Administrator
Step 8: Else
Step 9: Return Query.. Accepted
Step 10: End If
Step 11: Else
Step 12: Return Query.. Rejected
Step 13: End If
Step 14: End For
Step 15: End Procedure

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905193 |

V. RESULTS

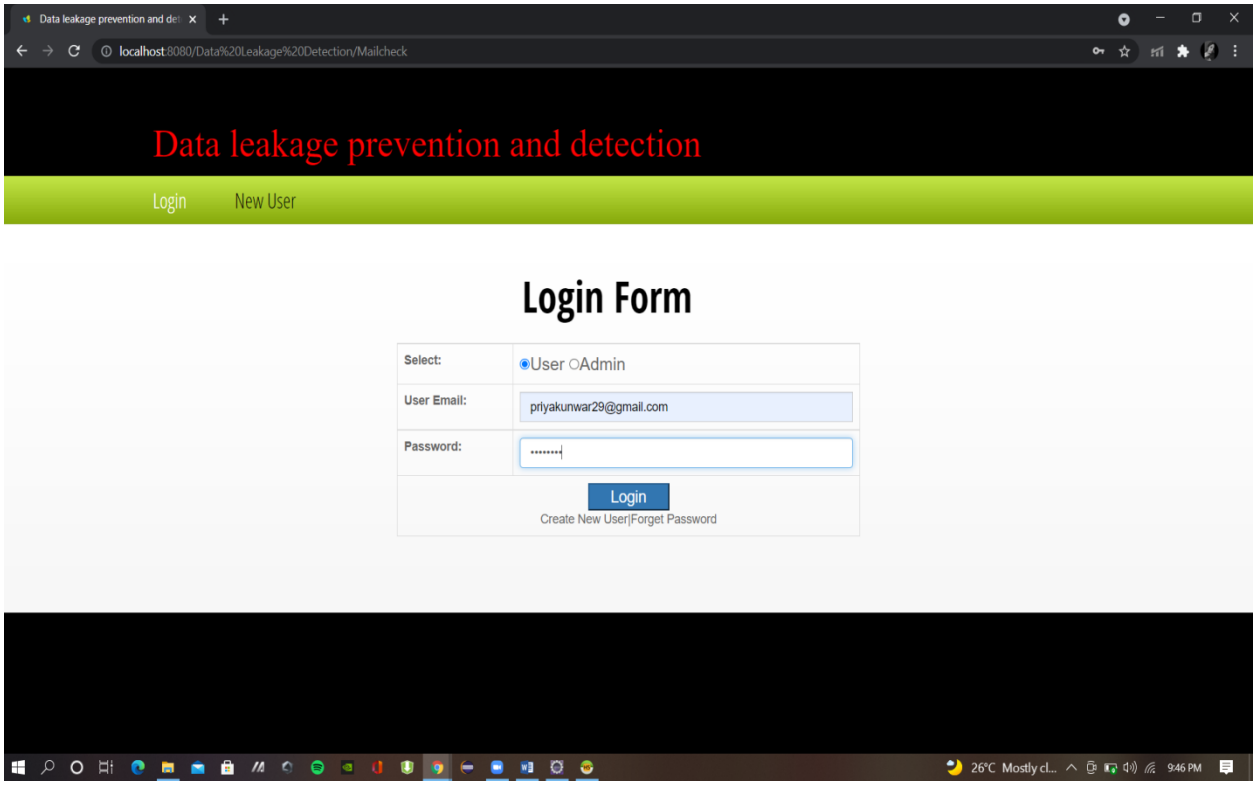


Fig 1: User Login Form

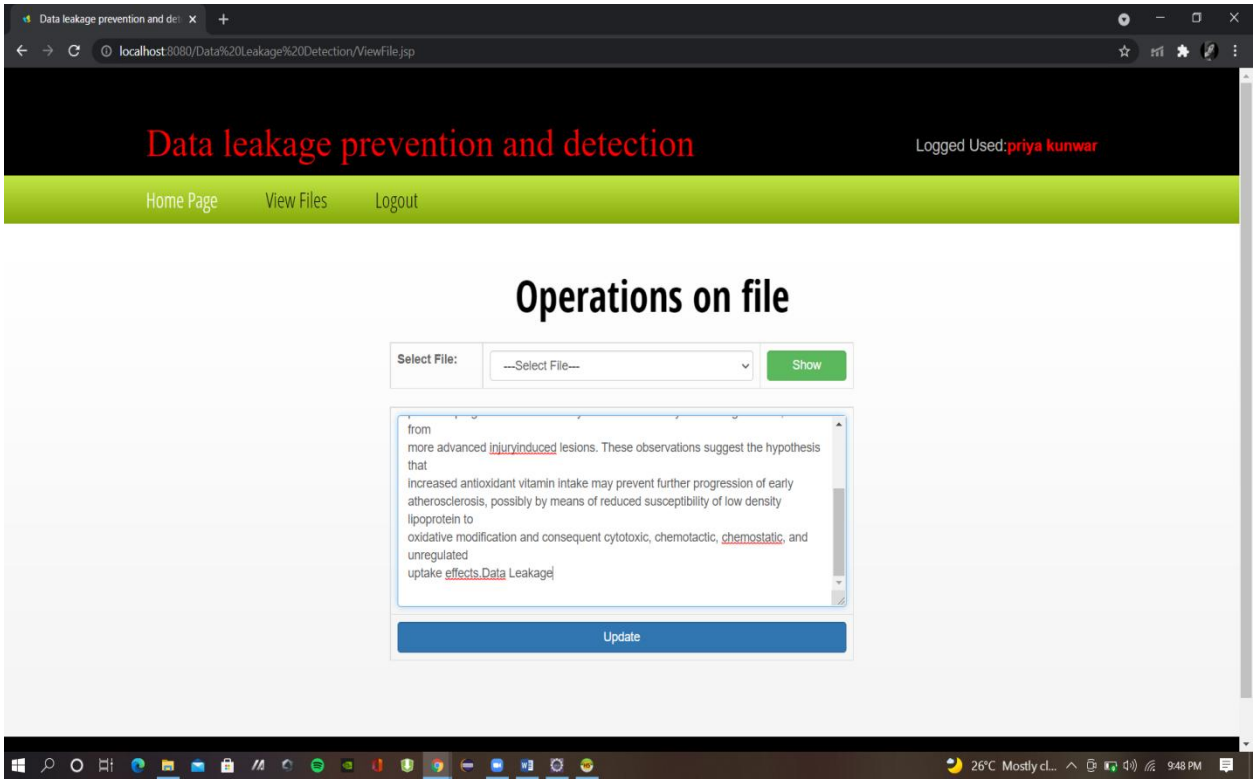


Fig 2: Updating of File by User (Attacker)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905193 |

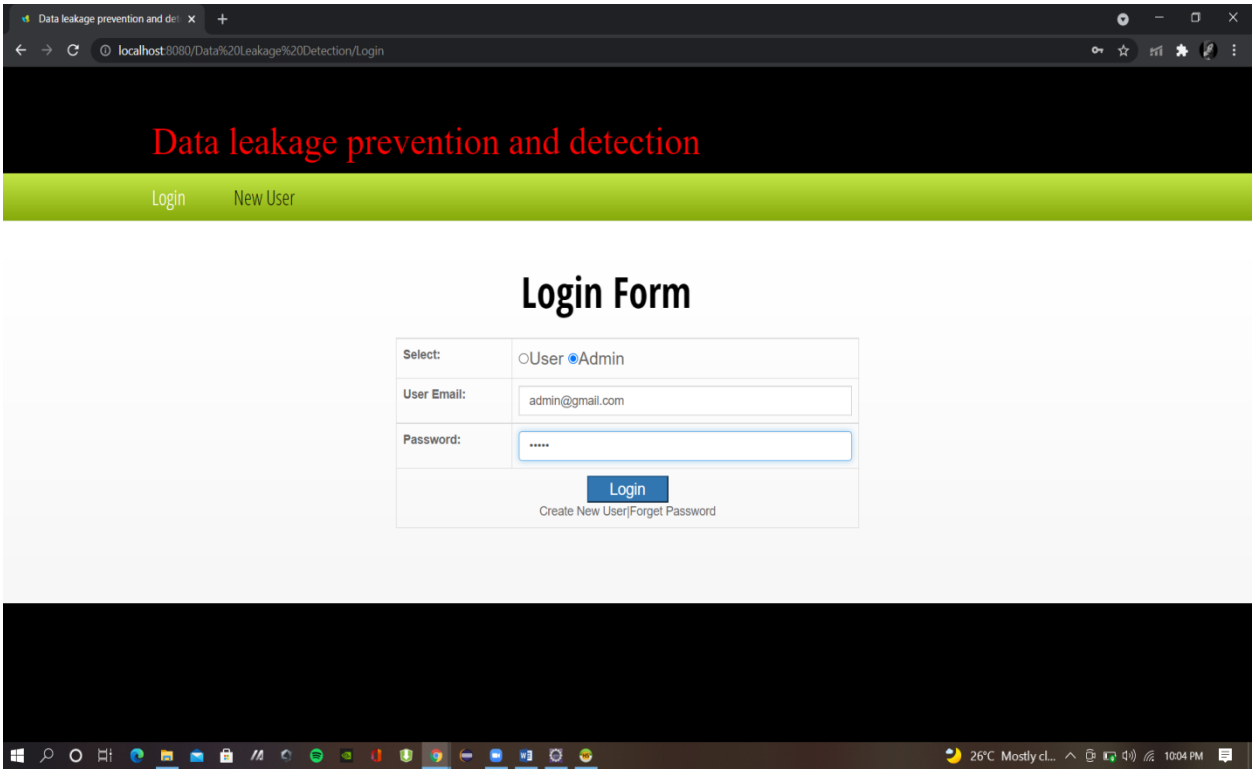


Fig Fig. 3: Admin Login Form

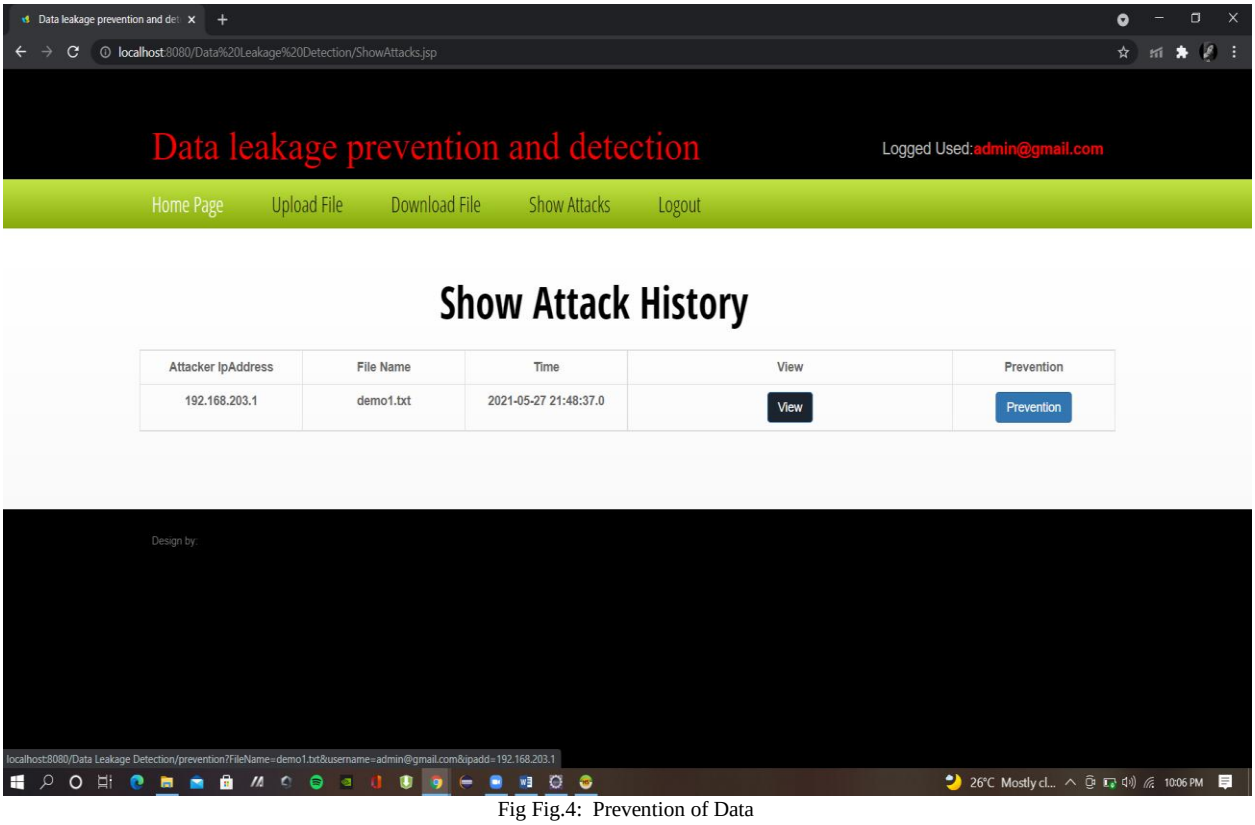


Fig Fig.4: Prevention of Data

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905193 |

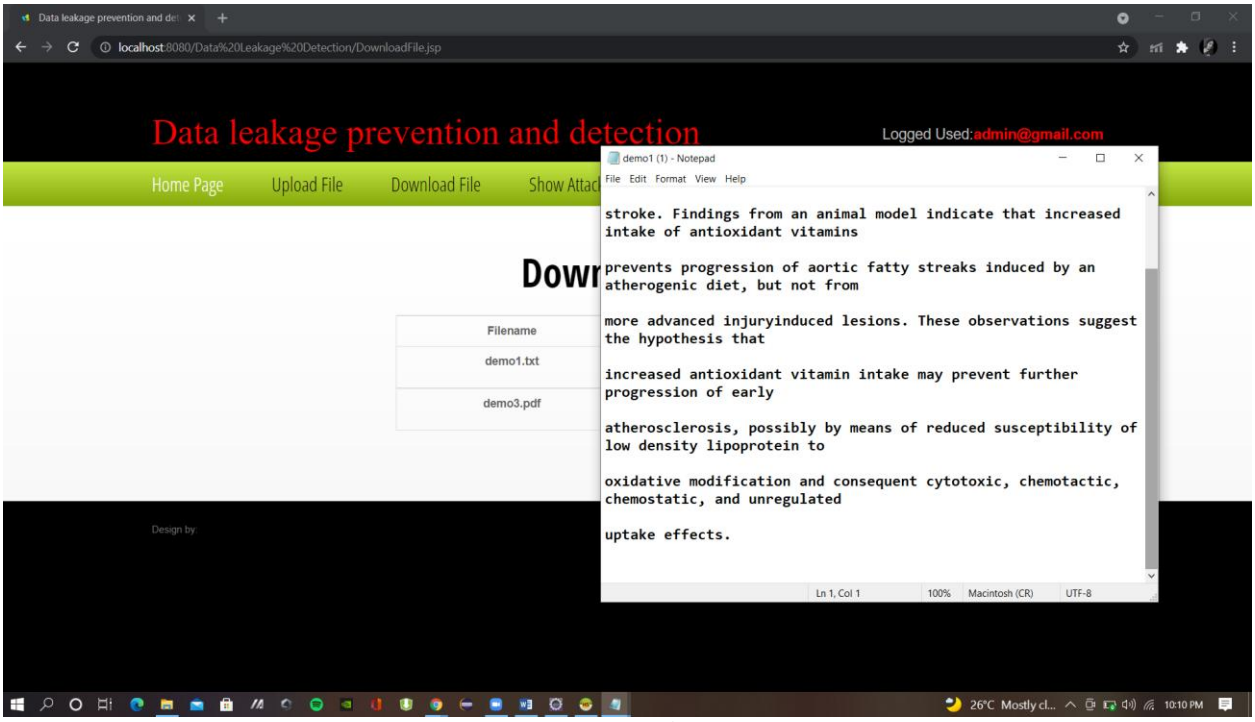


Fig Fig.5: Restoration of Original File

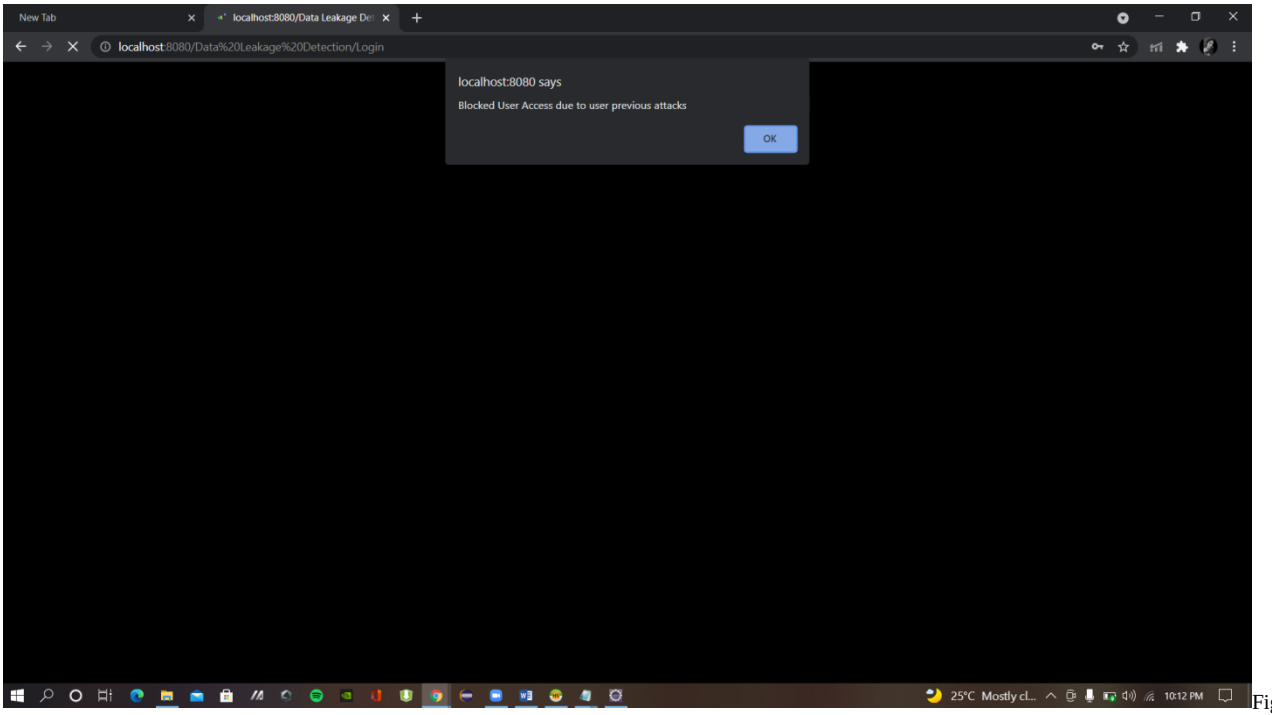


Fig.6: Blocked User Access due to user previous attack

VI. CONCLUSION AND FUTURE WORK

These studies show that, in terms of data leakage is a quiet but devastating risk.The confidential information may be lost without any knowledge. This may be done by an insider or an outsider. Sensitive data must be protected from the models of security analysis and design of secure computer systems, the security community has begun to implement a data mining, and a variety of techniques in order to discover the past. The unknown Attacks, Intrusion Detection

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905193 |

System (IDS), and Intrusion Prevention Systems (IPS) are commonly used to protect the network from cyber-attacks. The information, leak detection system, the model is very useful in relation to an existing watermark to a model. We are able to ensure the safety of our duties when it is distributed or transmitted, even if we have to detect when this happens. In other words, a security and tracking system was developed with the help of this model. The watermark can be simple to provide security through the use of a variety of encryption algorithms, this model provides peace of mind, plus, a detection method. Our model is relatively simple, however, we believe that this reflects a significant discount. Our proposed algorithms to implement a variety of data distribution strategies that can increase the chances of a distributor to detect any leak. We have shown that an efficient allocation of objects, could affect the identification of the responsible agents, in particular in those cases in which the information is to be obtained by the agents, which is very much the same. Our future work includes the study of the sin of the agent of the models, the sign of the leak scenarios.

FUTURE WORK

In the future, system will use email as showing data leakage detection and the snapshot will be send to admin respective mail. System will support camera as central for data prevention.

REFERENCES

1. Yin, Fan, Wang, Lina, Yu Rongwei, Ma, Xiaoyan, "A model for distribution, in order to avoid information leaking out," in 2013 IEEE International Conference on Mechatronic Sciences, a Global Engineering and Computer (MEC 2013), Wuhan, China.
2. Yadav Gitanjali, B., Bhaskar, P. S., Kamat, R. K., "Estimating the probability of a shame in a design-information leak", the 2012 International Journal of Computer Science and information technology.
3. Sushilkumar N. Kholambe, Ulhas, B. Shinde, Archana, There. Bhosale's Method "to determine who is to blame, it's the information leakage is found to be", 2015, International Journal of Computer Applications.
4. Dr. A. R. Pon, Periyasamy, Э. Thenmozhi "Dataleakage detection systems, and Data prevention Of the Algorithm" (2017), International Journal of Advanced Research in computer science and software engineering.
5. S. Praveen Kumar, Y. Srinivas, D. Suba Pao, Ashish Kumar, "A new Model for Data Leakage detection and Prevention in a Distributed Environment," In 2016 International Journal of Engineering and Technical Research (IJETR).

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details