International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 485-487 www.ijaem.net ISSN: 2395-5252

Advanced Data Leakage Prevention

Gaurang Shirsat[1], Manali Yadav[2], Anirudha Kale[3], Vinita Bhandiwad[4]

[1,2,3] *Students of Department of Information Technology, Vidyalankar Institute of Technology, Mumbai, Maharastra*

[4] *Prof. of Department of Information Technology, Vidyalankar Institute of Technology, Mumbai, Maharastra*

Submitted: 01-05-2021 Revised: 09-05-2021 Accepted: 10-05-2021

ABSTRACT: Nowadays there is a lot of use of Gmail and mailing sites to transfer the data from one person to another or from one organization to another. As we know there are hackers keeping a watch on the activities done by the organization or the specific person. The hackers track all the data going out as well coming to the organization or the person. This leads to data loss in which the important data of the organization or the person may be lost and to overcome this loss of important data we have come up with the idea of Advance Data Leakage Prevention web application.

Key Words: Hackers, data loss, Data leakage prevention, web application

I. INTRODUCTION

The main goal of our project is to stop the leakage of datafrom the person or an organization.In our project we will create an application which will help the user to login and register and that will help the sender and the receiver to create a private channel between them for communication. The methodology we are going to use comprises of Steganography, Cryptography and Random token generation. Steganography will be used for hiding the information into files or numbers, while the Cryptography will be used during the transmission and reception of the data over the channel, where it will check if the tokens match each other and if they match then the private channel will be active for communication or else we will come to know that the third party is trying to gain access. The random token generation mechanism will help us to generate a random token every time the user wants to send the data. This application will broadly help the organizations to send and receive confidential and important information without the fear of data leakage

1.1 AIM AND OBJECTIVE

The main objective of the proposed system is to create a private channel between the sender and the receiver to allow them to transfer and receive important and confidential information before the data being lost or any leakage in the data. This will help many organizations to transfer data over the internet without the fear of the data being lost or stolen. Aim of proposed system 1. Identify critical data: First, User must recognize how to identify their own critical data. This means being able to categorize what data is in need of the most protection and how to utilize data loss prevention (DLP) software to protect any sensitive information. 2. Monitor access and activity: The next step in preventing data leakage is to closely monitor traffic on all networks. Using Authentication and encryption provides broader protection. 3. Endpoints security: To provide securities to Users data and information by creating log systems.

1.2 LITERARTURE SURVEY

Ramadhan Mstafa, Christian Bach in paper [1] "Information hiding using steganography has reviewed Some Techniques for Steganography using this technique we will be able to hide the information that the user will send over to the other side. The information will be hidden and will not able to be decrypted by the third party.

Teamviewer GmbH in paper [2] "Team Viewer Security Statement" published the security policies.

The security mechanism provided by team viewer will help us in making the connection between the connection between the two parties secure and the connection cannot be penetrated.

Stjepan Gros in paper [3] "Security Risk Assessment of Team Viewer Application" has aim to risk assessment. There are many applications that provide a base for the transmission of the data, but all of them used public channels while team viewer uses private channel that is best suited for our application and can be used from anywhere after logging into the application.

Alpa Agath, Chintan Sidpara, Darshan Upadhyay in paper [4] "Critical Analysis of

Cryptography and Steganography" has proposed security analysis. This analysis helped us to understand the use of cryptography and various cryptographic standards that can be used for information hiding and the encryption and decryption of data.

1.3 ABOUT PROJECT

Data leakages are not only done using online mediums, electronic communication and services, and emails but also accidental data breach i.e. when an internal Sender sends a message, he or she may wrongly type a wrong ID or recipient name while sending the email.

Physical data leakage, malicious intent in Electronic communication such kinds of threats are real and need adequate actions to protect this data from getting leaked.

The proposed system will use random key generation algorithm for authentication and then creating the key using which data is encrypted before sending it to receiver. For online data sending mode we are using SHA algorithm and for offline mode we are using AES algorithm. For security of sending the data on the channel, steganography technique is used to hide the data and the same process will followed for decrypting the data on the receiver side.

It is a web application in which the user has to run before sending any important or confidential data to the client or any third party. After the user starts with the application the login/sign up page will be popped up and the user has to fill in the required information.

As the User_1 logs in to the application the random id for the user is created and then random token is generated at the back end which is then mapped with the random id created after that the user selects the data to be transmitted and with the help of SHA algorithm the encryption token for the data to be encrypted is generated and then with the of the key exchange algorithm we transfer the data to the intended recipient and the data send to the recipient is the encrypted data which needs to be decrypted with the help of the same algorithm and the recipient too has to login into the application and follow the same procedure after which the applications check if both the tokens are matching and if they match then the data is transmitted over the channel. Since the data is transmitted over a private channel and a unique random key is always generated the attacker will not able to find out the token number generated and the data always remains safe.

II. SCOPE OF RESEARCH

For any project to be successful, it is necessary that it will, satisfy all the requirements of the user. The user must feel comfortable with the system when he/she is using it. To achieve this, the system describes the scope of the project which should be accomplished within the deadline. If it achieves all the requirements, then system will be considered as successful. Scope for any project can be local or global.

2.1 LOCAL SCOPE:

The proposed system ADLP is based on organizations or groups of organizations for secure transfer and communication between them. Our application is user friendly, cost effective and applicable in real-time. By this approach the user can securely share the application with the fear of the data getting breached. It hasset all policies of single corresponding to each and every transmission, authenticated users and the secure share of data. This application can also be used in parts- if we want only online transmission of data

2.2 GLOBAL SCOPE:

The global scope of system will deal with newer modules and tasks to be integrated and implemented in nearby future of project development and maintenance cycles.

As there are limited facility available for the organizations, ADLP provides the right facility to the organizations for the secure transmission of confidential data. Web application is trending technology in the market and as our technology advances, it can only expect to see more come out of this system to benefit for the organizations.

III. SYSTEM OVERVIEW:

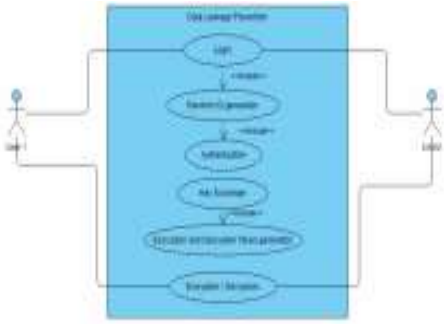
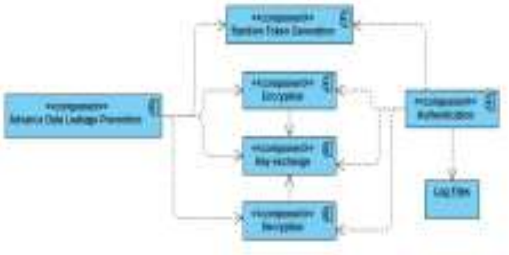


Fig 1: UML Diagram

The UML Diagram shows the flow of the project wherein how the data will be transferred.


«component» Random Token Generation
«component» Encryption
«component» Advance Data Leakage Prevention
«component» Authentication
«component» Key exchange
Log Files
«component» Decryption

IV. METHODOLOGY:

Data prevention is implemented for end to end on stable internet connection

1. User starts with the application the login/sign up page will be popped up and the user has to fill in the required information.

2. As the User logs in to the application the random id for the user is created and then random token is generated at the back end

3. Token is then mapped with the random id created 4. after that the user selects the data to be transmitted and with the help of SHA algorithm the encryption for the data to be generated

5. Use of the key exchange algorithm we transfer the data to the intended recipient and the data send to the recipient

6. The encrypted data which needs to be decrypted with the help of the same algorithm and the recipient too has to login into the application and follow the same procedure

7. After the applications check at backend if both the tokens are matching and if they match then the data is transmitted over the channel.

Since the data is transmitted over a private channel and a unique random key is always generated.

V. ACKNOWLEDGEMENT

We are pleased to present "Advanced Data Leakage Prevention" as our project and take this opportunity to express our profound gratitude to all those people who helped us in completion of this project. We thank our college for providing us with excellent facilities that helped us to complete and present this project. We would also like to thank the staff members and lab assistants for permitting us to use computers in the lab as and when required. We express our deepest gratitude towards our project guide Prof. Vinita Bhandiwadfor her valuable and timely advice during the various phases in our project. We would also like to thank her for providing us with all proper facilities and support as the project coordinator. We would like to thank her for support, patience and faith in our capabilities and for giving us flexibility in terms of working and reporting schedules. Finally, we would like to thank everyone who have helped us directly or indirectly in our project.

REFERENCES:

[1]. Ramadhan Mstafa, Christian Bach "Information hiding using steganography" Published in Northeast Conference of the American Society for Engineering Education in March 2013 https://www.researchgate.net/publication/259893801_Information_Hiding_in_Images_Using_Steganography_Techniques

[2]. Teamviewer GmbH "Team Viewer Security Statement" published the security policies. https://static.teamviewer.com

[3]. Stjepan Gros in "Security Risk Assessment of Team Viewer Application" published in Int. conference on Information Technology Interfaces has aim to risk assessment in June 2011 https://static.teamviewer.com

[4]. Alpa Agath, Chintan Sidpara, Darshan Upadhyay "Critical Analysis of Cryptography and Steganography" published in International Journal of scientific research of science, engineering and technology in 22 Jan 2018 http://www.derfrosch.de/msc/ic3-sheet09.pdf

[5]. Data Leakage (Data exchange) https://www.youtube.com/watch?v=2kp8M_eCsSs&feature= youtu.be