International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 195-200 www.ijaem.net ISSN: 2395-5252

Keystroke with Data Leakage Detection for Secure Email Authentication

T.Geetha M.E., M.B.A,[1] Assistant Professor, K.Baby, [2]n.Haritha, [3]r.P.Sowmiya[4]

Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur.

Submitted: 10-06-2021 Revised: 23-06-2021 Accepted: 26-06-2021

ABSTRACT: User authentication is considered to be an important aspect of any cyber security program. However, one-time validation of user's identity is not strong to provide resilient security throughout the user session. In this aspect, continuous monitoring of session is necessary to ensure that only legitimate user is accessing the system resources for entire session. In this paper, a true continuous user authentication system featuring keystroke dynamics behavioral biometric modality has been proposed and implemented. A novel method of authenticating the user on each action has been presented which decides the legitimacy of current user based on the confidence in the genuineness of each action. The 2-phase methodology, consisting of ensemble learning and robust recurrent confidence model (R-RCM), has been designed which employs a novel perception of two threshold i.e., alert and final threshold. Proposed methodology classifies each action based on the probability score of ensemble classifier which is afterwards used along with hyper parameters of R-RCM to compute the current confidence in genuineness of user. System decides if user can continue using the system or not based on new confidence value and final threshold. However, it tends to lock out imposter user more quickly if it reaches the alert threshold. Moreover, system has been validated with two different experimental settings and results are reported in terms of mean average number of genuine actions (ANGA) and average number of imposter in terms of mean average number of genuine with experimental settings.

I. INTRODUCTION

1.1 NETWORK SECURITY

A key area in security research is authentication, the determination of whether a user should be allowed access to a given system or resource. The important aspect of authentication is confidentiality and integrity. Also, for protecting any resource adequate authentication is the first line of defences. Here, for protection of resource use authentication as a service. It is important that the same authentication technique should not be used in every situation. A complication is that users may have many passwords for Bank, network and web sites. The large number of passwords increases interference and it is lead to forgetting or confusing passwords. The acceptability of any authentication scheme greatly depends on its robustness against attacks as well as its resource requirement both at the client and at the server end. It means authentication scheme require processing at client and server end.

1.1.1 Password Authentication

While password authentication is the most common way to confirm a user's identity, it isn't even close to the most effective or secures method.Anyone with your credentials could access your account without your permission, and the system wouldn't stop them. Most passwords are weak, and hacking techniques can break them in less and less time.

1.1.2 Email Authentication:

Email authentication is a password less option that allows users to securely log in using just an email address. The process is very similar to signing in with a Facebook or Twitter account, but this method offers a universal approach.

- **The user clicks the login button.** This opens a mailto link that directs the person to pre-written email that includes an encrypted token.
- **The user sends the email.** The message already comes with a recipient address so the user doesn't need to enter any information.
- **The server verifies the request.** Using a combination of token-based security checks, the user's identity is verified.

1.1.3 Biometric Authentication:

Biometric authentication includes any type of authentication method that requires a user's biology. While this may seem like new-age technology, you're probably already using it to unlock the screen on your smartphone. Fingerprint

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 195-200 www.ijaem.net ISSN: 2395-5252

scanning is the most well-known form of biometric authentication, but face recognition tools are an increasingly popular choice for developers.Of course, hackers have a **much** more difficult time replicating a users' biological characteristics, but it is important to note that these authentication processes are often less secure than you'd initially assume. Small fingerprint scanners on smartphones only record portions of your fingerprint, for instance.

II.LITERATURE SURVEY

2.1 Title: "A Novel Behaviour Profiling Approach To Continuous Authentication For Mobile Applications"

Authors: Alotaibi, Saud, Abdulrahman Alruban, Steven Furnell, And Nathan L. Clarke

Present a novel behavioural profiling approach to user identity verification as part of mobile application security. This work presented a novel behavioural profiling approach to verifying the user in terms of mobile application security and providing robust user identification. In this proposed work, three supervised machine learning algorithms were selected to evaluate the proposed approach and to determine the ideal classifier based on EER value. The experimental results show that the significance of this research lies in having successfully applied continuous user verification for mobile applications in a manner that fulfils both security and usability requirements. Although the authentication decision is based on action resolution, the experimental results are still promising. Making an authentication decision on each user action might lead to an unusable system which does not present transparent authentication.

ADVANTAGE

- With other people's work relevant to the focus of your study
- Provide efficient authentication using key stroke analysis

DISADVANTAGE

- Possible to data leakage in email environment.
- Password are hacked by third party

2.2 TITLE: "Double Serial Adaptation Mechanism For Keystroke Dynamics Authentication Based On A Single Password"

Authors: Mhenni, Abir, Estelle Cherrier, Christophe Rosenberger, And Najoua Essoukri Ben Amara

Propose a double serial adaptation strategy that considers a single-capture-based enrolment process. When using the authentication system, the template of users and the decision/adaptation thresholds are updated. Indeed, the user introduces the password only once, when creating a new account. Thus, the reference is composed of a single sample. Afterwards, for each successful authentication, the reference is updated in a transparent way. Avoiding the enrolment phase, the growing window mechanism serves to increase the size of the reference to capture more intra-class variations. Once the size of the reference reaches 10 samples, the sliding window will be considered in order to limit the number of samples saved in the reference. Consider a pre-processing step which intends to eliminate the noise in the captured characteristics.

ADVANTAGE

- Less time consumption for key generation and distribution
- Authorized person are only allowed to access mail

DISADVANTAGE

- Scalability is less
- To a comparative

III. EXISTING SYSTEM

Email is used by millions of people to communicate around the globe and is a critical application for Many businesses. Email messages passes through intermediate computers before reaching their final Destination and it is relatively easy for attackers to intercept and read messages. The backups of these Can remain up to several months on their server, even if we delete them from our mailbox.

Email is used by millions of people to communicate around the globe and is a critical application for Many businesses. Email messages passes through intermediate computers before reaching their final Destination and it is relatively easy for attackers to intercept and read messages. The backups of these Can remain up to several months on their server, even if we delete them from our mailbox.

Email is used by millions of people to communicate around the globe and is a critical application for Many businesses. Email messages passes through intermediate computers before reaching their final Destination and it is relatively easy for attackers to intercept and read messages. The backups of these Can remain up to several months on their server, even if we delete them from our mailbox.

Email is used by millions of people to communicate around the globe and is a critical application for Many businesses. Email messages passes through intermediate computers before

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 195-200 www.ijaem.net ISSN: 2395-5252

reaching their final Destination and it is relatively easy for attackers to intercept and read messages. The backups of these Can remain up to several months on their server, even if we delete them from our mailbox.

Email is used by millions of people to communicate around the globe and is a critical application for Many businesses. Email messages passes through intermediate computers before reaching their final Destination and it is relatively easy for attackers to intercept and read messages. The backups of these Can remain up to several months on their server, even if we delete them from our mailbox.

Nowadays an email is becoming a mainstream business tool. Email is used by millions of people to communicate around the world and it is important application for many businesses. An email is being used for communication at workplace and from social media logins to bank accounts. Authentication of the email process only processed with the help of username and password. User should create account and register their username and password for further verification process. Security of an email is the main concern for companies & it includes confidentiality that ensures information will not expose to unauthorized entities. Email messages passes through intermediate computers before reaching their final destination and it is easy for attackers to intercept and read messages. An email can be misused to leave sensitive data open to compromise. So, it may be of little surprise that attacks on emails are common. When an authenticated user leaves a system logged in and with a password attached to it that invites an attacker to steal the sensitive data at their leisure. If employee used that computer for personal use which means information is now willingly available to the attacker.

3.2 DISADVANTAGES

- Possible to data leakage in email environment.
- Anyone can read the message once they are logged into email application.
- Passwords are hacked by third party.
- No way to predict unauthorized data access in current email application.

V.MODULE DESCRIPTION

5.1 IMPLEMENTATION

To maintain authenticity and integrity of an email, here proposed an Email Protection System. Proposed EPS consider two parameters i.e. key stroke authentication and leakage detection. In many companies there are sensitive departments that consists sensitive information and they have right to send any information outside of the network. Proposed EPS will automatically check all outgoing mails from the sales department and take action based on what the administrator has specified in the policy. A distributor can maintain highly secure framework for email sharing process. A new user can be registered by entering personal details with email id and password. A registered user can login and make a message to forward to the receiver. The enhanced authenticated uses key stroke verification process. The system then extracts the data from the main database and performs the verification process to predict the fake records to the set of original records. It then provides this data to the receiver. The server may pass on this data to an unauthorized party. The agent or the unauthorized party may leak the sensitive data on the email. Whenever the distributor discovers the leaked set of his data, he will note the objects present in it. To prevent the leakage of data, implement key sharing method to verify the users. When a user receives the message through this mail.

5.2 LIST OF MODULES

- Email Framework Construction
- User Enrolment
- Keystroke Authentication
- Data Sharing
- Data leakage detection

5.2.1 Email Framework Construction

A mail server (also known as a mail transfer agent or MTA, a mail transport agent, a mail router or an Internet mailer) is an application that receives incoming e-mail from local users (people within the same domain) and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. In this module we can create the framework like as mail server. This framework contains server and multiple users. Server can maintain all user details. Users easily upload the files in inbox and also share the data anywhere and anytime.

5.2.2User Enrolment

In this Email application User has to register the appropriate details in the Email server database for using the authentication process. These details include user name, address, email id, contact number, primary password, confirm password and keystroke value. The key stroke value analysed during password typing. Keystroke duration threshold and user details are stored in the server database.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 195-200 www.ijaem.net ISSN: 2395-5252

5.2.3 Keystroke Authentication

Anonymous access is the most common web site access control method, which allows anyone to visit the public areas of a website while preventing unauthorized users from gaining access to a critical features and private information of web servers. The user verification phase analyses the mail id, password, keystroke value to the server. During password verification, key stroke time for password will be calculated and matched with database. User should enter the password with the specified time, otherwise they will not allow to access application.

5.2.4 Data Sharing

User can share the message to another user in secure email environment. Once completion of authentication process they will be allow to compose the mail. Then add the recipient detail to communicate. Receiver also creates account with key stroke authentication method. Authorized users are allowed to access this application.

5.2.5 Data leakage detection

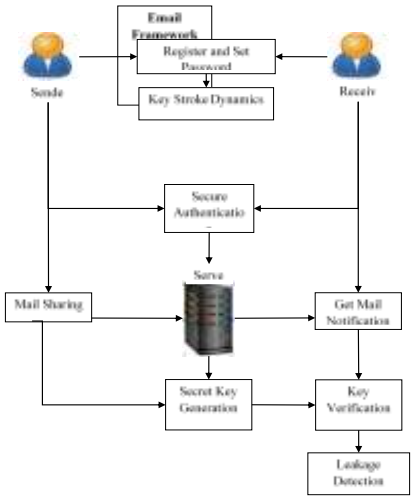
The Mail is being sent to authorized user and unauthorized user. As the unauthorized user receives the mail, the system detects that the mail has been send to the unauthorized user using key verification process; Receiver want to verify their secret key before accessing mail content. Here, on the user side, if the unauthorized user accesses that mail, the mail does not display the contents of the mail.

VI. SYSTEM DESIGN

6.1 SYSTEM ARCHITECTURE

System architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability. System architecture must describe its group of components, their connections, interactions among them and deployment configuration of all component.

SYSTEM ARCHITECTURE



VII.SOFTWARE DESCRIPTION

7.1.1 FRONT END: PHP

PHP: Hypertext Pre-processor (the name is a recursive acronym) is a widely used, general-purpose scripting language that was originally designed for web development to produce dynamic web pages. For this purpose, PHP code is embedded into the HTML source document and interpreted by a web server with a PHP processor module, which generates the web page document. As a general-purpose programming language, PHP code is processed by an interpreter application in command-line mode performing desired operating system operations and producing program output on its standard output channel. It may also function as a graphical application. PHP is available as a processor for most modern web servers and as standalone interpreter on most operating systems and computing platforms. PHP was originally created by RasmusLerdorf in 1995 and has been in continuous development ever since. The main implementation of PHP is now produced by The PHP Group and serves as the de facto standard for PHP as there is no formal specification. PHP is free software released under the PHP License, which is incompatible with the GNU General Public License (GPL) because restrictions exist regarding the use of the term PHP. Hypertext refers to files linked together using hyperlinks, such as HTML

7.1.2 Accessing an HTML Page

Fig 3.1 Accessing an HTML page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 195-200 www.ijaem.net ISSN: 2395-5252

Your browser sends a request to that web page's server (computer) for the file (HTML or image) you wish to view.

1. The web server (computer) sends the file requested back to your computer.
2. Your browser displays the file appropriately.
3. If you request a PHP file (ends with ".php"), the server handles it differently.

7.2 ACCESSING A PHP PAGE

Fig 3.2 Accessing a PHP Page

1. Your browser sends a request to that web page's server for the PHP file you wish to view.
2. The web server calls PHP to interpret and perform the operations called for in the PHP script.
3. The web server sends the output of the PHP program back to your computer.
4. Your browser displays the output appropriately.

7.3BENEFIT OF PHP

Because the server does processing, the output of PHP files changes when its input changes. For example, most of the pages on the Horticulture site have only two (2) PHP commands:

1. Include the header file that defines the links on the left, the banner, and the quick links at the top.
2. Include the footer file that displays the mission statement and Horticulture contact information.

VIII.TESTING

8.1 SOFTWARE TESTING

Software testing is a method of assessing the functionality of a software program. There are many different types of software testing but the two main categories are dynamic testing and static testing. Dynamic testing is an assessment that is conducted while the program is executed; static testing, on the other hand, is an examination of the program's code and associated documentation. Dynamic and static methods are often used together.

Testing Objectives:

- There are several rules that can serve as testing objectives, they are
- Testing is a process of executing a program with the intent of finding an error
- A good test case is one that has high probability of finding an undiscovered error.
- A successful test is one that uncovers an undiscovered error.

The development process involves various types of testing. Each test type

• Unit Test.
• Functional Test
• Integration Test
• White Box Test
• Block Box Test

8.1.1 UNIT TESTING

The first test in the development process is the unit test. The source codeis normally divided into modules, which in turn are divided into smaller units called units. These units have specific behaviour. The test done on these units of code is called unit test. Unit test depends upon the language on which the project is developed. Unit tests ensure that each unique path of the project performs accurately to the documented specifications and contains clearly defined inputs and expected results.

8.1.2 FUNCTIONAL TESTING:

Functional test can be defined as testing two or more modules together with the intent of finding defects, demonstrating that defects are not present, verifying that the module performs its intended functions as stated in the specification and establishing confidence that a program does what it is support

8.1.3 INTEGRATION TESTING:

In integration testing modules are combined and tested as a group. Modules are typically code modules, individual applications, source and destination applications on a network, etc. Integration Testing follows unit testing and precedes system testing...

8.1.4 WHITE BOX TESTING:

Testing based on an analysis of internal workings and structure of a piece of software. This testing can be done sing the percentage value of load and energy. The tester should know what exactly is done in the internal program. It includes techniques such as Branch Testing and Path Testing.

8.1.5 BLACK BOX TESTING:

In black box testing tester have without knowledge of the internal workings of the item being tested. Tests are usually functional. This

testing can be done by the user who has no knowledge of how the shortest path is found.

IX. CONCLUSION AND FUTURE ENHANCEMENT

9.1 CONCLUSION

To deal with the problem of Data leakage, we have presented implementation a variety of data distribution strategies that can improve the distributor's chances of identifying a leaker. Also we have implemented the concept of key stroke authentication for user authentication. In proposed email framework users register using their details with key stroke values. During login process, user can also verified using their password with key stroke values. This will enhance the process of authentication in email. Also provide OTP generation, to predict the authorization of user during email content access.

9.2 FUTURE ENHANCEMENT

Future work includes the investigation of agent guilt models that capture leakage scenarios. Also Implement Watermarking that uses various algorithms through encryption to offer security, whereas probability-based model provides both the security as well as detection technique to identify guilty.