International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 3, March-April 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Keystroke with Data Leakage Detection for Secure Email Authentication

Mrs. V. Hemalatha[1], V. Boominathan[2], K. Harithas[2], P. Raj Kumar[2], S. Vijaya Bharathi[2]

[1]HOD,
[1,2]Department of CSE, N.S.N. College of Engineering and Technology, Karur, Tamil Nadu, India

## ABSTRACT

The user authentication is the important factor which allows the user to use a particular software. The user authentication is also performed in various kinds of social media such as Gmail, Facebook, etc. The traditional password system is used for user authentication. But this technique has a lot of demerits in it. Some hackers also cracks the password and perform some unwanted actions in the user authentication. In order to remove the difficulties in this traditional password technique and to provide additional security in user authentication, the keystroke with data leakage detection for secure email authentication is designed. This system uses Keystroke Dynamics. This system consists of five different types of modules such as Email Framework Construction, User Enrolment, Keystroke Authentication, Data Sharing and Data Leakage Detection. This system gets the details of the user such as name and email. Then it allows to enter the password. This password is stored along with the keystroke dynamics data such as the typing speed of the password and the threshold value. Both the Keystroke dynamics data and the original password are stored in the database. When the user wants to log into the system, the user has to give the password according to the keystroke dynamics data. Then only, the user can log into the system. Hence this system can also be used in Cyber security and provide security and privacy for the user data.

***KEYWORDS***: *Responsive, Mobility, Keystroke Dynamics, security*

***How to cite this paper***: Mrs. V. Hemalatha | V. Boominathan | K. Harithas | P. Raj Kumar | S. Vijaya Bharathi "Keystroke with Data Leakage Detection for Secure Email Authentication" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-3, April 2021, pp.797-799, URL: www.ijtsrd.com/papers/ijtsrd39969.pdf

IJTSRD39969

## 1. INTRODUCTION

Authentication is one of the most important process. One of the oldest technique in protecting the user data is to use passwords. But nowadays, passwords are easier to crack and there is no protection for user's data. Hence, the Keystroke Dynamics feature is used to enhance the security features and the user authentication of a system.

### 1.1. PROBLEM STATEMENT

The major problem in most of the IT companies are Data leakage and cracking of passwords. Most of the Hackers use password cracking softwares to crack the user's password and perform some unwanted actions such as stealing the data, modifying the data and add some unwanted data with the user's data. This causes more number of problems in all kinds of fields.

## 2. OBJECTIVES

The goals of our project is to create a system which uses keystroke dynamics for user authentication.

- The user interface of this system should be efficient, user friendly and maintain privacy.
- This system should provide security against all kinds of piracy.
- This system should notify the user when the data of the user has been hacked.

## 3. EXISTING SYSTEM

Email is used by millions of people to communicate around the world and it is important application for many businesses. The backups of these can remain up to several months on their server, even if it is deleted the mailbox. Nowadays an email is becoming a mainstream business tool. An email is being used for communication at workplace and from social media logins to bank accounts. Authentication of the email process is 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.

## 4. PROPOSED SYSTEM

Email is one of the crucial aspects of web data communication. The increasing use of email has led to a lucrative business opportunity called spamming. To overcome the problems of authentication and data leakage in email sharing provide key stroke authentication technique and random key sharing methods. Keystroke authentication can be classified as either static or continuous. The static refers to keystroke analysis performed only at specific times, for example during the login process. When the latter is applied, the analysis of the typing speed is performed continuously during the whole session, thus providing a tool to detect user substitution after the login. Proposed work has implemented based on static key stroke method. In the enrolment phase, for each user, a threshold based key stroke values are acquired. Leakage detection is implemented using key sharing through SMS. When the message was shared between sender and receiver, secret key will be generating and distributing to the authority. When a receiver wants to view the shared message, they will be authenticate using key value. Otherwise unauthorized access notification is shared to the authority.

### 4.1. ARCHITECTURE

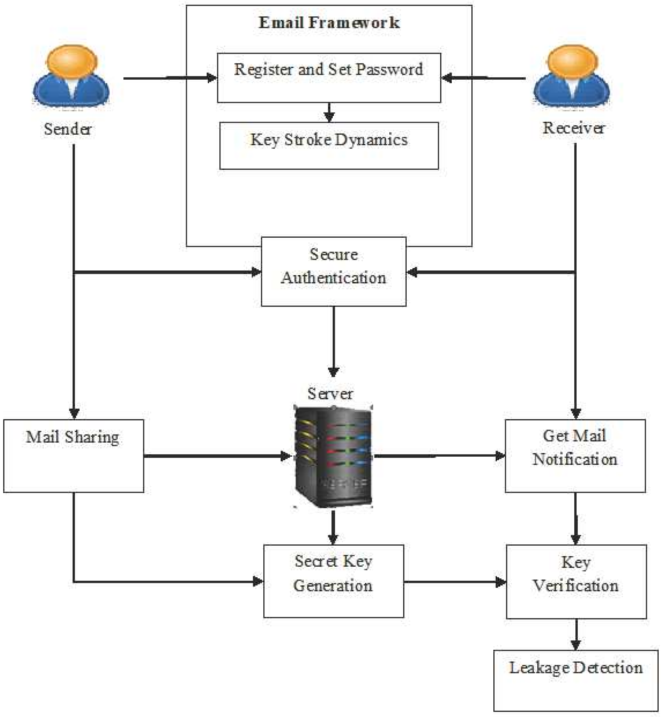

**Fig.1 System Architecture**

## 5. FIELDS OF THIS SYSTEM

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

### 5.1. Email Framework Construction

A mail server is an application that receives incoming e-mail from local users 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 framework like a mail server was created. 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. This framework enable for provide key stroke authentication and leakage detection process.

### 5.2. User 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 username, address, email id, contact number, primary password, confirm password and keystroke value. The key stroke value analyzed during password typing. Keystroke duration threshold and user details are stored in the server database.

### 5.3. Keystroke Authentication

Anonymous access is the most common website 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 analyzes the mail id, password and keystroke value of 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.

### 5.4. 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.

### 5.5. 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.

## 6. CONCLUSION

To deal with the problem of Data leakage, this system implements a variety of data distribution strategies that can improve the distributor's chances of identifying a leaker. Also it includes implementation of 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 be verified using their password with key stroke values. This will enhance the process of authentication in email and also provides OTP generation, to predict the authorization of user during email content access.

### 6.1. Future Enhancement

Future work includes the investigation of agent guilt models that capture leakage scenarios. Watermarking that uses various algorithms through encryption to offer security can be designed along with probability-based model which provides both the security as well as detection technique to identify guilty.

## REFERENCES

[1] Alotaibi, Saud, Abdulrahman Alruban, Steven Furnell, and Nathan L. Clarke. "A Novel Behaviour Profiling Approach to Continuous Authentication for Mobile Applications." In ICISSP, pp. 246-251. 2019.

[2] Mhenni, Abir, Estelle Cherrier, Christophe Rosenberger, and Najoua Essoukri Ben Amara. "Double serial adaptation mechanism for keystroke dynamics authentication based on a single password." Computers & Security 83 (2019): 151-166.

[3] Foresi, Andrew, and Reza Samavi. "User authentication using keystroke dynamics via crowd

sourcing." In 2019 17th International Conference on Privacy, Security and Trust (PST), pp. 1-3. IEEE, 2019.

[4] Salem, Asma, and Mohammad S. Obaidat. "A novel security scheme for behavioral authentication systems based on keystroke dynamics." Security and Privacy 2, no. 2 (2019): e64.

[5] Ferrari, Carlo, Daniele Marini, and Michele Moro. "An adaptive typing biometric system with varying users model." In 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 564-568. IEEE, 2018.

[6] Shen, Sung-Shiou, Tsai-Hua Kang, Shen-Ho Lin, and Wei Chien. "Random graphic user password authentication scheme in mobile devices." In 2017 International conference on applied system innovation (ICASI), pp. 1251-1254. IEEE, 2017.

[7] Alsuhibany, Suliman A., Muna Almushyti, Noorah Alghasham, and Fatimah Alkhudier. "Analysis of free-text keystroke dynamics for Arabic language using Euclidean distance." In 2016 12th International Conference on Innovations in Information Technology (IIT), pp. 1-6. IEEE, 2016.

[8] Ahmed, Ahmed A., and Issa Traore. "Biometric recognition based on free-text keystroke dynamics." IEEE transactions on cybernetics 44, no. 4 (2013): 458-472.

[9] Huang, Jiaju, Daqing Hou, and Stephanie Schuckers. "A practical evaluation of free-text keystroke dynamics." In 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), pp.1-8. IEEE, 2017.

[10] Senathipathi, K., and Krishnan Batri. "An analysis of particle swarm optimization and genetic algorithm with respect to keystroke dynamics." In 2014 international conference on green computing communication and electrical engineering (ICGCCEE), pp. 1-11. IEEE, 2014.