Keylogger- Innovative Keystroke Dynamics And Ensuring Secure Email Authentication

GirishtharunU[1], Visweshwaran A[2], Manoranjan V[3], Dr. R. Shobarani[4], Ms. Subbulakshmi[5]
[1, 2, 3] Dept of B.sc ISCF
[4]Professor
[5]Assistant Professor
[1, 2, 3, 4, 5] Dr.M.G.R Educational and Research Institute, Deemed to be University, Chennai.

Abstract- *Keystroke-dynamics based authentication is a cheap biometric mechanism that has been proven accurate in distinguishing individuals. We design and implement a simple and easy to-adopt protocol for authenticating a computer owner that utilizes the user's keyboard activities as an authentication metric. Keystroke dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to identify users based on habitual typing rhythm patterns. In this project, we can design the system for mail application to register their details such as user name and password. At the time of password typing, time is calculated for typing whole password and also calculates the time for typing each and every letter in password. The time duration is send to email in encrypted format. So hackers are difficult to extract details.*

I. INTRODUCTION

A key area in security research is authentication, the determination of whether a user should be allowed access to a given system or resource.[1] The important aspect of authentication is confidentiality and integrity. Also, for protecting any resource adequate authentication is the first line of defense. Here, for protection of resource we 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. To put it simply, authentication is the process that confirms a user's identity. Traditionally, this is done through a username and password. The user enters their username, which allows the system to confirm their identity; this system relies on the fact that (hopefully) only the user and the site's server know the password. The website authentication process works by comparing the user's credentials with the ones on file. If a match is found, the authentication process is complete.

II. REQUIREMENT ANALYSIS

2.1 OBJECTIVE OF THE PROJECT

The security threat to the network can be the attacker who attempts to grasp information to exploit the network vulnerability. This kind of attack is also known as passive attack. On the other hand, the attacker is attempting to disrupt the network communication and also affect the user productivity of a network.[2] It is also known as an active attack. Here listed below are some of the most common types of the security threats. 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 mail to 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.

2.2 EXISTING SYSTEM

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. [3]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.

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.

2.3 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 classier as either static or continuous.[4] 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 implementing 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 authenticate using key value. Otherwise unauthorized access notification shared to the authority.

Advantages

- Provide efficient authentication using key stroke analysis.
- Authorized persons are only allowed to access mails.
- Less time consumption for key generation and distribution.

III. REQUIREMENT SPECIFICATIONS

3.1 HARDWARE REQUIREMENTS

- Processor : Dual core processor 2.6.0 GHZ
- RAM : 2GB
- Hard disk : 160 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard
- Monitor : 15 inch color monitor

3.2 SOFTWARE REQUIREMENTS

- Operating system : Windows OS
- Front End : PHP
- Back End :MySQL SERVER
- IDE :Macromedia Dreamweaver
- Application :Web application

IV. MODULES

- Email Framework Creation
- User Enrolment
- Keystroke Authentication
- Content Sharing
- Mail Access

Email Framework Construction - 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.Users easily upload the files in inbox and also share the data anywhere and anytime.[5] This framework enable for provide key stroke authentication and leakage detection process.

User Enrolment - In this Email application User has to register the appropriate details in the Email server database for using the authentication process. The key stroke value analyzed during password typing. Keystroke duration threshold and user details are stored in the server database.

Keystroke Authentication - The user verification phase analyzes the mail id, password, keystroke value to the server. During password verification, key stroke time for password will be calculated and matched with database.[6] User should enter the password with the specified time, otherwise they will not allow to access application.

Content 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.Receiver also creates account with key stroke authentication method. Authorized users are allowed to access this application.

Mail Access - As the unauthorized user receives the mail, the system detects that the mail has been send to the unauthorized user using key verification process; [7]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.

V. ARCHITECTURE DIAGRAM

It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).

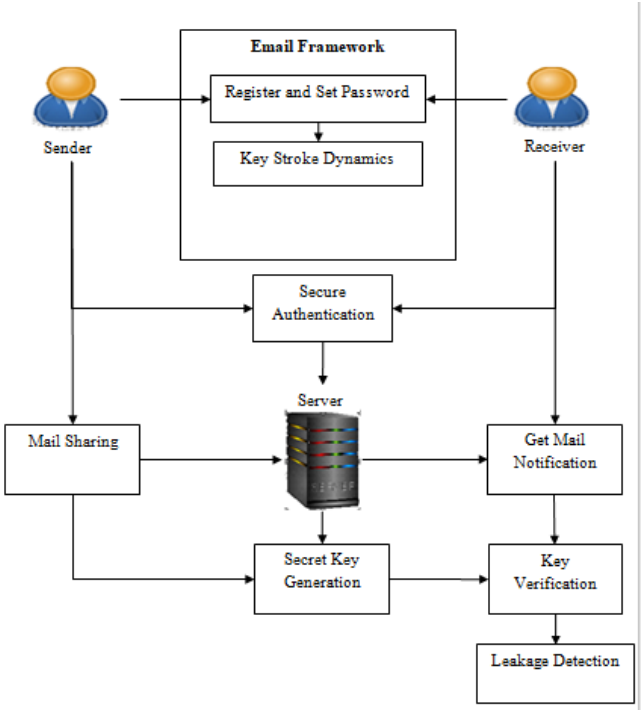

Fig no.1ARHITECTURAL DIAGRAM

VI. IMPLEMENTATION

Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the users, what it will work efficient and effectively.[8] It involves careful planning, investing of the current system, and its constraints on implementation, design of methods to achieve the changeover methods.[9]The coding step translates a detail design representation into a programming language Realization. Programming languages are vehicles for communication between human and computers programming language characteristics and coding style can profoundly affect software quality and maintainability. The coding is done with the following characteristics in mind.

- Ease of design to code translation.
- Code efficiency.
- Memory efficiency.
- Maintainability.

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective

VII. 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[10]. This will enhance the process of authentication in email. Also provide OTP generation, to predict the authorization of user during email content access. In future, extend the framework multimedia content analysis with duplicate detection. Multimedia content provides large data storage so that implement duplicate detection and also detect video based duplicate detection.

REFERENCES

[1] Çeker, H., &Upadhyaya, S. (2019, September). User authentication with keystroke dynamics in long-text data.In 2019 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-6).IEEE.

[2] Raul, N., Shankarmani, R., & Joshi, P. (2020). A Comprehensive Review of Keystroke Dynamics-Based Authentication Mechanism.In International Conference on Innovative Computing and Communications (pp. 149-162). Springer, Singapore

[3] Mhenni, Abir, et al. "Double Serial Adaptation Mechanism for Keystroke Dynamics Authentication Based on a Single Password." Computers & Security, vol. 83, 2019, pp. 151–166., DOI:10.1016/j.cose.2019.02.002.

[4] Alsultan, A., Warwick, K., & Wei, H. (2019). Non-conventional keystroke dynamics for user authentication. Pattern Recognition Letters, 89, 53-59.

[5] Krishnamoorthy, S., Rueda, L., Saad, S., &Elmiligi, H. (2018, May). Identification of user behavioural biometrics

for authentication using keystroke dynamics and machine learning.In Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications (pp. 50-57).

[6] Lin, C. H., Liu, J. C., & Lee, K. Y. (2020). On neural networks for biometric authentication based on keystroke dynamics. Sensors and Materials, 30(3), 385-396.

[7] Huang, J., Hou, D., &Schuckers, S. (2019, February). A practical evaluation of free-text keystroke dynamics. In 2019IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (pp. 1-8).IEEE.

[8] Zhang, J., Tan, X., Wang, X., Yan, A., & Qin, Z. (2018). T2FA: Transparent Two-Factor Authentication. IEEE Access, 6, 32677–32686

[9] Kochegurova, E. A., Gorokhova, E. S., &Mozgaleva, A. I. (2020, January). Development of the keystroke dynamics recognition system. In Journal of Physics: Conference Series (Vol. 803, No. 1, p. 012073).

[10] Nath, Asoke&Mondal, Tanushree. (2022). Issues and Challenges in Two Factor Authentication Algorithms. International Journal of Latest Trends in Engineering and Technology(IJLTET). 6. 318-327.