ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024

Behaviour Based User Authentication for Secure Communication System

[1] P. Bhuvaneshwari,B.Tech.,M.E., [2] K Keerthivasan, [3] S Meiyappan, [4] M Yogachandran
[1] Assistant Professor, Department of Information Technology,Muthayammal Engineering College (Autonomous),Rasipuram - 637 408, Tamil Nadu, India
Bhuvaneshwari.p.it@gmail.com
[2][3][4] Department of Information Technology Muthayammal Engineering College (Autonomous) Rasipuram - 637 408, Tamil Nadu, India
[2] vasankeerthi518@gmail.com, [3] meijack927@gmail.com, [4]Yoga8112002@gmail.com

Abstract: ***Keystroke-dynamics based authentication is a simple 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 verification techniques can be classified as either static or continuous. Static verification approaches analyze keystroke verification characteristics only at specific times, for example, during the login sequence. Static approaches provide more robust user verification than simple passwords, but do not provide continuous security they cannot detect a substitution of the user after the initial verification. Continuous verification, on the contrary, monitors the user's typing behavior throughout the course of the interaction. 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. So hackers are difficult to extract details. Also propose AES encryption method for end to end mail encryption process. These methods do not rely on alterations of the released data. Also implement OTP verification for accessing shared email it helps to further improve our chances of detecting leakage and identifying the guilty party. In a perfect world there would be no need to hand over sensitive data to agents that may unknowingly or maliciously leak it. And even if we had to hand over sensitive data, in proposed work implement secret key sharing method. Key will be verified before accessing the shared mail information. This will avoid the unwanted and malicious access of email data.***

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. 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. 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 sever end. Due to the proliferation of mobile and hand-held devices the resource requirement has become a major factor. The implicit passwords main application is the protection of critical resources and systems. Nowadays users can access any information including banking and corporate database with the use of mobile phones.

However, our proposal can also be used in other scenario where confidentiality and integrity are the major security requirements. We propose our Authentication System for banking using Implicit Password. in which the scheme allows any image to be used and it does not need artificial predefined click regions with well-marked boundaries – a password can be any arbitrarily chosen sequence of points in the image with some finer differences. In IPAS, the server has the piece of information i.e. password at the time of authentication and at the time of registration, the user give this information to the server in an implicit form. Implicit password is particularly suited for mobile phones and portable computers, although it may be implemented for any computer.

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. RELATED WORK

Smart- card-centered password authentication is likely one of the most handy and typically used two-factor authentication mechanisms. This technology has been greatly deployed in quite a lot of varieties of authentication applications which

incorporate far off host login, on-line banking and entry manipulate of constrained vaults, activation of protection contraptions, and lots of extra. A sensible-card situated password authentication scheme includes a server S and a customer A (with identity IDA). In the beginning, S securely issues a smart-card to A with the wise-card being personalized with admire to IDA and an initial password. This segment is referred to as the registration segment and is applied best as soon as for each customer. In a while, A can access S within the login-and-authentication phase, and this section will also be implemented as commonly as wanted. Nonetheless, in this section, there could have more than a few sorts of passive and active adversaries in the communication channel between A and S. They may be able to eavesdrop messages and even alter, dispose of or insert messages into the channel. The protection intention of the scheme in this segment is to be certain mutual authentication between A and S. In detailed, the purchaser is required to each have the sensible-card and comprehend the password with a purpose to carry out the wise-card-established password authentication effectively with server S. In other words, the scheme must furnish two-factor authentication.

III. PROPOSED ALGORITHM

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 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. OTP will be verified in reverse order verification process.When the encrypted message was shared between sender and receiver, secret key will be generating and distributing to the authority.Time based key sharing enables the receiver to get access within time limit.When a receiver wants to view the shared message, they will authenticate using key value. Otherwise unauthorized access notification shared to the authority.

ALGORITHM

Keystroke dynamics

- Keystroke features are usually obtained using the timing particulars of the key down or key hold or events.
- It is known by different names such as typing biometrics and typing rhythms.
- The main advantage of using keystroke dynamics is that it does not require any extra hardware.
- Two basic features used for keystroke dynamics are Key Hold time and Inter Key time.

AES Encryption

- The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages.
- This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it’s counterpart in the encryption algorithm.

ADVANTAGES

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

IV. PSEUDO CODE

The proposed secure email application helps to sharing information in secure manner. In this application enhancing the authentication factor using keystroke based authentication method. And implement a cryptography approach for secure message sharing.

LIST OF MODULES

- Email Framework Construction
- User Enrolment
- Keystroke Authentication
- Reverse OTP Verification
- Content Sharing
- Mail Access

MODULE DESCRIPTION

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. 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. These details include user name, 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.

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 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. User should enter the password with the specified time, otherwise they will not allow to access application.

Reverse OTP Verification

A One Time Password is a string of characters or numbers automatically generated to be used for one single login attempt. One Time Passwords can be sent to the user's phone via SMS is used to protect web-based services, private credentials and data. The risk of fraud is drastically reduced if the user doesn't only have to fill in his user name and password but also needs OTP have to complete the login. Here user should enter their OTP in reverse order. This will enhance the efficiency compared with existing OTP based authentication system.

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. Message could be encrypted using AES encryption algorithm. During secret key sharing content owner can set time control for key validation process. Authorized users are allowed to access this application.

Mail Access

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.

SYSTEM ARCHITECTURE

V. SIMULATION RESULTS

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 components.

The above figure explains the process of implementing a robust system involves a combination of innovative authentication methods and encryption protocols. Leveraging keystroke-based password authentication adds an extra layer of security, employing user-specific typing patterns to uniquely identify individuals during login. Further ensuring the confidentiality of email content, an advanced encryption mechanism is applied for secure sharing, safeguarding sensitive information from unauthorized access.

To fortify the process, a one-time-password (OTP) is sent to the recipient at the time of mail access; enhancing the verification process and ensuring that only authorized individuals can open and read the encrypted email. This comprehensive approach not only protects sensitive communications but also adheres to stringent security standards, providing a secure and trustworthy environment for email communication.

VI. IMPLEMENTATION

System implementation is the important stage of project when the theoretical design is tuned into practical system. The main stages in the implementation are as follows:

- Planning
- Training
- System testing and
- Changeover Planning

Planning is the first task in the system implementation. Planning means deciding on the method and the time scale to be adopted. At the time of implementation of any system people from different departments and system analysis involve. They are confirmed to practical problem of controlling various activities of people outside their own data processing departments. The line managers controlled through an implementation coordinating committee. The committee considers ideas, problems and complaints of user department, it must also consider;

- The implication of system environment
- Self-selection and allocation form implementation tasks
- Consultation with unions and resources available
- Standby facilities and channels of communication

VII. CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, an end-to-end encrypted email service using AES encryption and user authentication using keystroke dynamics is a secure way to protect user data and privacy. AES encryption is a widely accepted standard for encryption and provides strong protection against unauthorized access to email content. User authentication using keystroke dynamics is a biometric method that can help verify a user's identity and prevent unauthorized access to the email account. However, it is important to note that the security of the system depends not only on the encryption and authentication methods but also on the implementation of these methods. Therefore, it is crucial to have a well-designed system that takes into consideration potential vulnerabilities and employs security best practices. Overall, an end-to-end encrypted email service using AES encryption and user authentication using keystroke dynamics can provide a high level of security and privacy for email communication.

Keystroke dynamics can be time-consuming and may not be convenient for all users. Future work could focus on improving the user experience, for example by reducing the number of keystrokes required for authentication or developing alternative authentication methods that are faster and more user-friendly. Current email systems are often centralized, which can present security and privacy risks. Future work could explore the development of a decentralized email system that provides end-to-end encryption and user authentication, while also enabling users to maintain greater control over their data.

REFERENCE

[1] Belman, Amith K., and Vir V. Phoha. "DoubleType: Authentication using relationship between typing behavior on multiple devices." In 2020 International Conference on Artificial Intelligence and Signal Processing (AISP), pp. 1-6.IEEE, 2020.

[2] Belman, Amith K., and Vir V. Phoha. "Discriminative power of typing features on desktops, tablets, and phones for user identification." ACM Transactions on Privacy and Security (TOPS) 23, no. 1 (2020): 1-36.

[3] Chauhan, Jagmohan, Young D. Kwon, Pan Hui, and Cecilia Mascolo. "Contauth: Continual learning framework for behavioral-based user authentication." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 4, no. 4 (2020): 1-23.

[4] Acien, Alejandro, Aythami Morales, Ruben Vera-Rodriguez, Julian Fierrez, and John V. Monaco. "TypeNet: Scaling up keystroke biometrics." In 2020 IEEE International Joint Conference on Biometrics (IJCB), pp. 1-7.IEEE, 2020.

[5] Zhao, Qingchuan, ChaoshunZuo, Brendan Dolan-Gavitt, Giancarlo Pellegrino, and Zhiqiang Lin. "Automatic uncovering of hidden behaviors from input validation in mobile apps." In 2020 IEEE Symposium on Security and Privacy (SP), pp. 1106-1120.IEEE, 2020.

[6] Yang, Pan, NaixueXiong, and JingliRen. "Data security and privacy protection for cloud storage: A survey." IEEE Access 8 (2020): 131723-131740.
[7] Feng, Yao, Fan Wu, Xiaohu Shao, Yanfeng Wang, and Xi Zhou. "Joint 3d face reconstruction and dense alignment with position map regression network." In Proceedings of the European conference on computer vision (ECCV), pp. 534-551. 2018.
[8] Ferrari, Claudio, Stefano Berretti, and Alberrto Del Bimbo. "Extended youtube faces: a dataset for heterogeneous open-set face identification." In 2018 24th International Conference on Pattern Recognition (ICPR), pp. 3408-3413.IEEE, 2018.
[9] Lin, Yiming, Shiyang Cheng, JieShen, and MajaPantic. "Mobiface: A novel dataset for mobile face tracking in the wild." In 2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019), pp. 1-8.IEEE, 2019.
[10] Wang, Hao, Yitong Wang, Zheng Zhou, Xing Ji, Dihong Gong, Jingchao Zhou, Zhifeng Li, and Wei Liu. "Cosface: Large margin cosine loss for deep face recognition." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5265-5274. 2018.