IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.301

Volume 3, Issue 4, May 2023

Enhanced Authentication Method for Cryptography Based Communication System

Rebekha R[1], Naveen A[2], Sanjay V[3], Sivasubramaniyan A[4]

Assistant Professor, Department of Information Technology [1]

Students, B.Tech, Final Year, Depaetment of Information Technologyu [2,3,4]

Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

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. At specific times, for example, during the login sequence. 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 methodfor end to end mail encryption process. Also implement OTP verification for accessing shared email it helps to further improve our chances of detecting leakage and identifyingthe 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.

Keywords: Keystroke Verification , Biometric Machanism, Hackers, Encryption and Decryption, Security.

I. INTRODUCTION

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. 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 The implicit passwords main application is the protection of critical resources and systems. Nowadays users can access any information including banking and corporate databasewith the use of mobile phones.

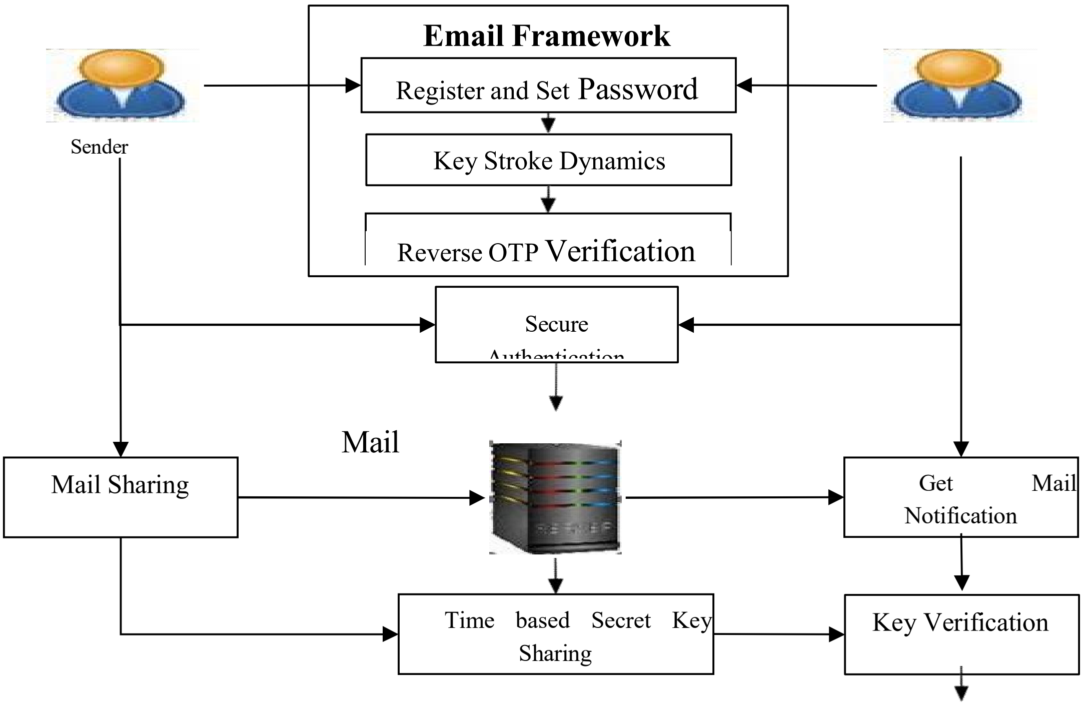
In which the scheme – a password can be any arbitrarily chosen sequence of points in the image with some finer differences. In IPAS, the serverhas the piece of information i.e. password at the time of authentication and at the time of registration, the user give this information to the server in an implicit form. To put it simply, authentication is the process that confirms a user's identity

Traditionally, this is done througha username and 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.

DOI: 10.48175/IJARSCT-9898

ISSN
2581-9429
IJARSCT

II. SYSTEM ARCHITECTURE



with architectural style and quality attributes. reliability, scalability, portability, and availability

III LIST OF MODULE

Email Framework Construction: A mail server (also known as a mail transfer agent or MTA, a mail transport agent, A computer dedicated to running such applications is also called a mail server. This framework contains server and multiple users. Server can maintain all user details. User share the data anywhere and anytime.

User Enrolment: In this Email application User has to register the appropriate details in the Email server database for using the authentication process

Keystroke Authentication: Anonymous access is the most common web site access control method, which allows and private information of web servers.

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. 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. 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 toaccess 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.

DOI: 10.48175/IJARSCT-9898

IV. SCREEN SHOTS

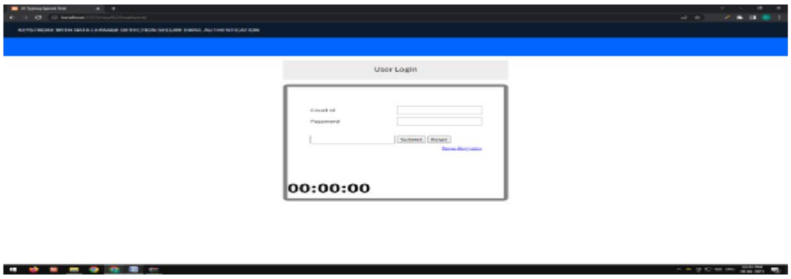
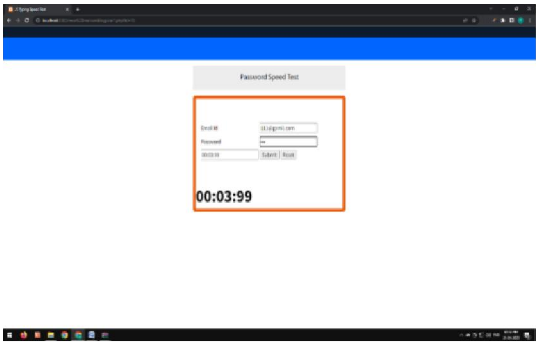


Fig 1: Home page



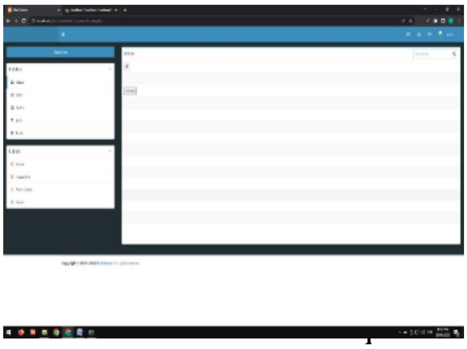


Fig 2: keystroke value storage Fig 3: User Home page

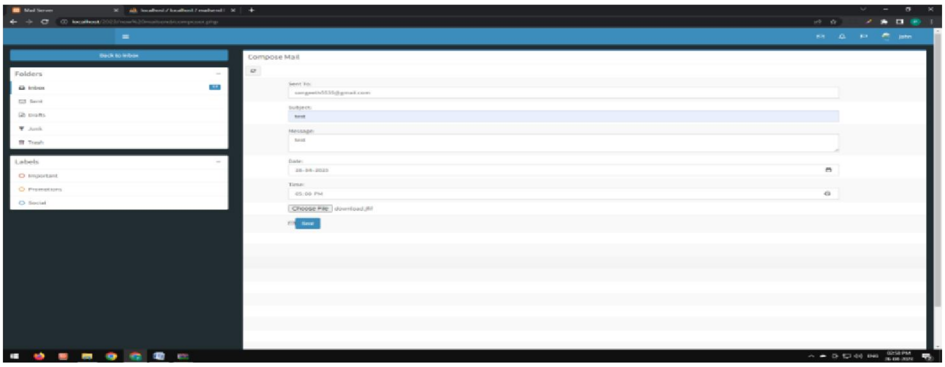


Fig 4: Compose mail

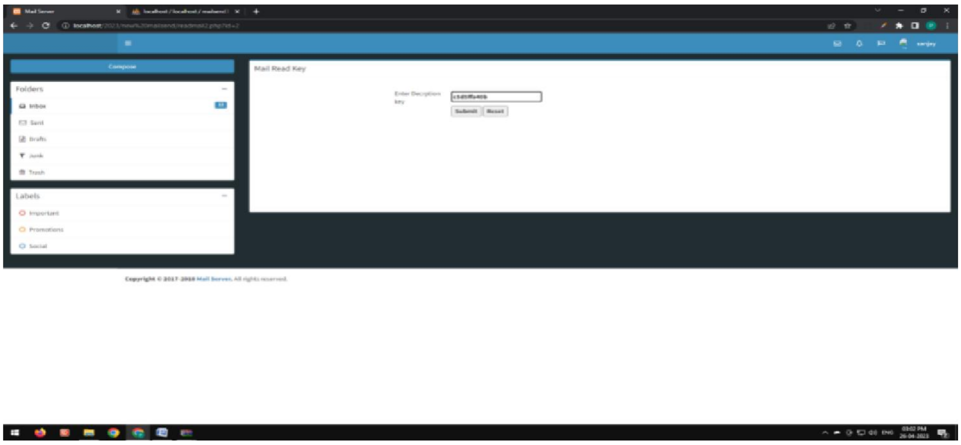


Fig 5:Key verification

DOI: 10.48175/IJARSCT-9898

V FUTURE ENHANCEMENT

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.

VI CONCLUSION

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 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. system that takes into consideration potential vulnerabilities and employs security best practices. Overall, an end-to-endencrypted email service using AES encryption and user authentication using keystroke dynamics can provide a high levelof security and privacy for email communication.

REFERENCES

[1] Shakya, Subarana. "An efficient security framework for data migration in a cloud computing environment." Journal of Artificial Intelligence 1, no. 01 (2019): 45-53.

[2] Yang, Pan, NaixueXiong, and JingliRen. "Data security and privacy protection for cloud storage: A survey." IEEE Access 8 (2020): 131723-131740.

[3] Seth, Bijeta, SurjeetDalal, VivekJaglan, Dac‐Nhuong Le, Senthilkumar Mohan, and GautamSrivastava. "Integrating encryption techniques for secure data storage in the cloud." Transactions on Emerging Telecommunications Technologies 33, no. 4 (2022): e4108.

[4] Li, Hongbo, Qiong Huang, JianShen, Guomin Yang, and Willy Susilo. "Designated-server identity-based authenticated encryption with keyword search for encrypted emails." Information Sciences 481 (2019): 330-343.

[5] Abera, Tigist, RaadBahmani, Ferdinand Brasser, Ahmad Ibrahim, Ahmad-Reza Sadeghi, and Matthias Schunter. "DIAT: Data Integrity Attestation for Resilient Collaboration of Autonomous Systems." In NDSS. 2019.

[6] Wei, Jianghong, Wenfen Liu, and Xuexian Hu. "Secure data sharing in cloud computing using revocable-storage identity- based encryption." IEEE Transactions on Cloud Computing 6, no. 4 (2016): 1136-1148.

[7] Phuong, Tran Viet Xuan, Willy Susilo, Jongkil Kim, Guomin Yang, and Dongxi Liu. "Puncturable proxy re-encryption supporting to group messaging service." In Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I 24, pp. 215-233. Springer International Publishing, 2019.

[8] Sun, Shi-Feng, Amin Sakzad, Ron Steinfeld, Joseph K. Liu, and DawuGu. "Public-key puncturable encryption: modular and compact constructions." In Public-Key Cryptography–PKC 2020: 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4–7, 2020, Proceedings, Part I 23, pp. 309-338. Springer International Publishing, 2020.

[9] Garg, Sanjam, Mohammad Hajiabadi, Mohammad Mahmoody, and AhmadrezaRahimi. "Registration-based encryption: removing private-key generator from IBE." In Theory of Cryptography: 16th International Conference, TCC 2018, Panaji, India, November 11–14, 2018, Proceedings, Part I 16, pp. 689-718. Springer International Publishing, 2018.

[10] Abu-Salma, Ruba, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, AlenaNaiakshina, and Matthew Smith. "Obstacles to the adoption of secure communication tools."In 2017 IEEE Symposium on Security and Privacy (SP), pp. 137- 153.IEEE, 2017.

DOI: 10.48175/IJARSCT-9898
ISSN 2581-9429 IJARSCT

BIOGRAPHY

Dr.RRebekha,.M.E,Ph.D..,Assistant Professor, Department of Information Technology, 14 Years of Experience , Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Thiruvarur-614 403

Mr.A.Naveen , Pursuing B.Tech – Information Technology (IT) Final Year in Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Thiruvarur-614 403

Mr.V.Sanjay, Pursuing B.Tech – Information Technology (IT) Final Year in Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Thiruvarur-614 403

Mr.A.Sivasubramaniyan, Pursuing B.Tech – Information Technology (IT) Final Year in Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Thiruvarur-614 403

DOI: 10.48175/IJARSCT-9898

ISSN
2581-9429
IJARSCT
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY