Multi-Factor Authentication using NDB for Robust Protection

Visali C[1], Radha S[2], Ashmitha P[3], Yamini Aruna M[4]
B.Tech-Information Technology.
Vivekanandha College of Engineering for women

ABSTRACT - Numerous well-known Internet applications have been introduced as a result of technological advancements. E-banking, or mobile banking, is one such vital program that significantly affects our contemporary lives. While banks promote internet banking as a safe and secure way to interact, there is actually a significant risk involved. Despite this, banks actively encourage their consumers to conduct business online. Increased expenses and security risks have been brought about by the spread of mobile banking apps, which has made stronger security protocols more expensive for customers and banks alike. There are several different techniques to hack a mobile banking system, including phishing, botnets, Trojan horses, and more. Multifactor authentication systems are available to confirm the legitimacy of the client; nevertheless, their disadvantage lies in the fact that they operate at the transaction level instead of the authentication level. This creates the opportunity for so-called man-in-the-middle attacks to occur between users and browser security systems, smartphones, etc. It is now essential to establish a more practical and practicable approach based on the transaction cum authentication level for mobile banking security. This paper attempts to suggest an authentication that improves the security of online banking systems. We suggest a hybrid one-time password that uses SHA 256 bit random OTP.

Keywords: MFA, Cloud Infrastructure, Authentication Factors, Cloud Security, Cloud Computing

INTRODUCTION

With the increasing prevalence of cloud infrastructure and cybersecurity concerns, it is more important than ever to protect digital ecosystems from unauthorized access. The growing trend of enterprises shifting their operations to the cloud has made sensitive data more vulnerable and attractive to potential attackers. As a crucial defensive strategy, multifactor authentication (MFA) has arisen in response to this changing threat scenario. By using multiple authentication factors, like biometrics, tokens, or device-based authentication, MFA adds an extra layer of protection to the conventional dependence on passwords alone. The goal of this methodical survey is to thoroughly investigate and assess the variety of multifactor authentication techniques designed with cloud infrastructure in mind. It explores several techniques, technologies, and implementations to provide a thorough overview of the state of MFA in the context of cloud security. It also provides insights into the advantages, disadvantages, and new developments in protecting digital assets in the ever-changing world of cloud computing.

1.1 MULTIFACTOR AUTHENTICATION (MFA)

Multifactor Authentication (MFA) prevents unauthorized access to systems and applications by requiring users to provide multiple forms of identity. Multi-factor authentication (MFA) adds extra layers of verification, usually combining two or more authentication factors, in contrast to standard single-factor authentication techniques that just use passwords. These variables frequently consist of the user's knowledge (passwords, for example), possessions (security tokens, smartphones, etc.), and identity (biometric information, such as fingerprints or face recognition). MFA dramatically improves the security posture of systems by adding numerous stages of authentication, reducing the possibility of unwanted access and shielding sensitive data from potential breaches. Protecting against ever- evolving cybersecurity threats is critical in a variety of digital contexts, including cloud infrastructure, where the use of multifactor authentication (MFA) has become increasingly important.

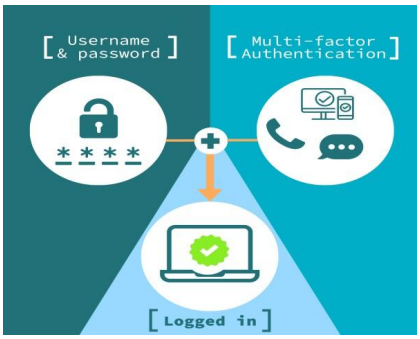


Figure 1. MFA

CLOUD INFRASTRUCTURE

Cloud infrastructure is a disruptive force in the ever-evolving world of modern technology, altering the conventional paradigms of computing and data administration. Cloud infrastructure, which is different from traditional on-premises solutions, uses the internet's power to provide a scalable and adaptable platform for the delivery of computing resources, services, and applications. Cloud infrastructure is an advanced collection of virtualized servers, storage systems, networking components, and security measures that enables enterprises to operate digital processes more effectively by overcoming the constraints of physical hardware. Cloud infrastructure has become the foundation of contemporary IT systems, enabling innovation, cost optimization, and agility and ushering in a new era of accessibility, adaptability, and computational efficiency. It also makes seamless service delivery possible. This introduction lays the groundwork for a thorough examination of the complex world of cloud infrastructure, where the convergence of connection and technology is redefining how individuals, organizations, and governments use computer resources to achieve a range of goals.

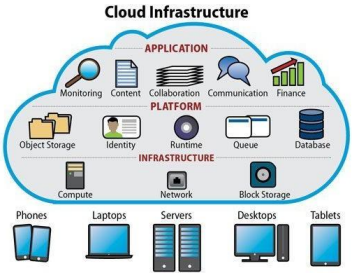


Figure 2. Cloud Infrastructure

1.2 AUTHENTICATION FACTORS

The protection of private data and safe access to online resources have become critical issues in the ever-growing digital world. Strengthening the integrity of digital interactions is largely dependent on authentication, which is the process of confirming the identity of users or systems. The foundation of this verification procedure is made up of authentication elements, which are divided into three categories: "something you know," "something you have," and "something you are." The use of passwords as the only form of authentication has proven insufficient in the face of growing cyber threats. As a result, multifactor authentication (MFA), or the integration of several authentication factors, has become an essential tactic to enhance security measures. This investigation explores the many domains of authentication factors, from possession-based components like tokens and advanced biometric identifiers to knowledge- based credentials like passwords. Organizations may strengthen their digital perimeters, guaranteeing strong protection against

illegal access and cultivating a more resilient security posture in our networked and data-driven environment, by comprehending and utilizing these complex aspects.

1.3 CLOUD SECURITY

As more and more businesses realize how revolutionary cloud computing can be, it is critical to protect digital environments from constantly changing cyberattacks. The cornerstone of this effort is cloud security, which is made up of an extensive collection of procedures, tools, and guidelines intended to safeguard information, programs, and infrastructure housed on the cloud. Scalability, flexibility, and accessibility are the main draws of cloud services, but these benefits also pose significant risks to the availability,confidentiality, and integrity of digital assets. There is a vast array of cloud security solutions available, ranging from network security and compliance frameworks to identity management and encryption. This investigation explores the complexities of cloud security with the goal of elucidating the tactics and tools that support the safeguarding of confidential data in cloud environments. This study of cloud security is an essential resource for businesses navigating the challenging landscape of protecting their data and operations in the rapidly developing field of cloud computing in an era characterized by fast digital transformation.

LITERATURE REVIEW

1.4 A BIOMETRIC AUTHORIZATION AND SEARCHABLE ENCRYPTION SCHEME FOR CLOUD ENVIRONMENTS

In this research, Marius Iulian Mihailescu [1] et al. claim that cloud computing offers the ability of giving a collection of resources appropriate access within a network. In order to save and minimize the usage of local storage and other resources, many users outsource their data to various cloud services. One of the main issues is the storage of private information on distant servers, which can be quite difficult in various contexts involving privacy. In addition to being a specific example of Fully Homomorphic Encryption (FHE), Searchable Encryption (SE) is a technique made up of a number of algorithms designed to safeguard sensitive user data while maintaining server-side searching capabilities. A set of algorithms called Searchable Encryption (SE) is used in this technique. developed to preserve server-side searching capabilities while protecting sensitive user data. SE mostly comes in two varieties: A limited number of users possess the public key necessary for them to output ciphertexts and enable the creation of trapdoors with the holder's private key thanks to Public Key Searchable Encryption (PKSE).

Searchable Symmetric Encryption (SSE) uses private key holders to perform cipher texts and trapdoors for searching. In this work, we propose a searchable encryption system based on biometric authentication. Furthermore, the trapdoor creation process uses biometric data to prevent unauthorized users from submitting search queries. Three parts make up the proposed system: biometric authentication, searchable encryption technique, and traditional user authentication (password, username, and code message sent via short message service [SMS]). The first two components can be thought of as two-factor authentication (2FA), while the second component represents the searchable encryption system's initialization process.

1.5 A CLOUD-CAPABLE INDUSTRIAL SMART VEHICLES WITH AN ATTRIBUTE-BASED ACCESS CONTROL

According to Maanak Gupta [2] et al.'s proposal in this research, linked industrial vehicles that provide users with cognitive and data-driven services are a key component of the smart city idea. This kind of communication among distributed linked objects is sometimes called the Industrial Internet-of-Vehicles (IIoV). The main goals of Intelligent Transportation Systems (ITS) are to protect driver safety and provide users with a comfortable experience. However, adversaries can remotely exploit and control essential mechanics in smart vehicles, such as the engine and brake systems, because to these intricate infrastructures' wide attack surfaces. The widespread adoption of this ground-breaking technology is seriously hampered by security and privacy issues until the whole vision of ITS is fully realised. ln order to offer a formal Attribute-

Based Access Control framework and address access control issues in the HoV ecosystem. (sometimes referred to as ITS-ABACG), this study is an initial step this research. Groups are introduced in the proposed model and assigned to different smart entities according to their qualities. Moreover, it offers system-wide regulations for accepting or rejecting alerts, cautions, and adverts from different connected smart entities. Moreover. It respects each person's right to privacy and enables the development of fine-grained security regulations.

1.6 MOBILE DEVICES: USER AUTHENTICATION APPROACHES, THREATS, AND TRENDS

In this study, Chen Wang [3] et al. make the point that having access to a variety of apps on mobile devices including online shopping has significantly improved our degree of convenience. Connect to mobile media, banking, and navigation from anywhere at any time. While going "Go Mobile" gives consumers convenience and flexibility, there's a chance that private data held on mobile devices like names and credit card numbers could be hacked. By unlocking the devices, an attacker could gain access to the private and sensitive data kept on them. Furthermore, all of the user's mobile services and applications include some level of security risk. Using the user's mobile device, for example, the adversary may engage in illegal acts (such installing malware and making purchases online). keeping private user information safe on mobile devices. Protecting sensitive user data on mobile devices and preventing unauthorized access are two major purposes of mobile device authentication. This study examines the current mobile device authentication techniques. To be more accurate, we categorize the existing mobile authentication techniques into four groups: two- factor authentication, physiological biometric (fingerprint and iris), behavioral biometrics (gait and hand gesture), and knowledge-based (passwords and lock patterns). Based on the basic authentication measures (knowledge, ownership, and biometrics) employed in various techniques, these groups have been established. The basic authentication metrics (knowledge, ownership, and biometrics) employed in these techniques

form the basis of these categories. Among these areas, we contrast the security and usefulness of the current authentication methods. In addition, we examine the current attacks against various authentication strategies in order to identify their weaknesses.

1.7 INTERNET BANKING IN THE WILD: A SURVEY OF MULTI-FACTOR AUTHENTICATION

According to Federico Sinigaglia [4] et al.'s research, there has been a notable increase in the use of internet banking services in the last several years. Multi-factor authentication, or MFA, is being used by banks to protect the sensitive resources these services oversee from hackers. Thus far, banks have employed many multi- factor authentication (MFA) systems, each possessing distinct characteristics and layouts that provide varying levels of security and user experience. Public and private authorities have set rules and guidelines to aid in the creation of more secure and user-friendly MFA solutions, even if it is unclear how they will impact the MFA systems that are now in use. The design choices made in this work are suggested to be examined latitudinally. We provide here the findings of a long-term investigation into the design decisions made by global banks along with the way they implement MFA. In particular, we evaluate the MFA solutions now in use in the banking sector according to three criteria: (i) complexity; (ii) resilience to attacks; and (iii) conformity to legislative requirements and industry best practices. We also examine possible connections between these standards. Based on this inquiry, we highlight several lessons learned and outstanding issues. Over the last ten years, there has been an increase in the tendency towards internet-based businesses. Internet services are increasingly prevalent in the financial sector, with the majority of banks now offering online services.

1.8 SECURITY FAILURES IN COMPARING MULTI-FACTOR AUTHENTICATION SCHEMES FOR MULTI-SERVER ENVIRONMENTS

In this research, Ding Wang [5] et al. have suggested that the key to understanding how to achieve greater security is to reveal the security weaknesses of existing cryptographic protocols. For multi-server situations, dozens of multi- factor authentication techniques have been presented over time, however the majority have quickly been found to be problematic. This field's research trend has devolved into an unfavorable "break-fix-break-fix" cycle, wherein substantial efforts have been expended but minimal substantive advancements have been achieved. In this paper, we review five popular two-factor authentication schemes for multi-server environments and show that they are all lacking key features (like user anonymity) or have serious security flaws (like temporary information leakage attacks and the lack of truly multi-factor security).

2. EXISTING SYSTEM

It is necessary to take precautions against the misuse of the different cloud computing services and resources. The two biggest issues with cloud computing are authentication and access control. Numerous scholars in this domain propose various methods to improve cloud authentication in the direction of resilience. As Single Factor Authentication has been around for a while, user names and passwords have also. But as computing power has increased, so too have the use of low-tech techniques, such as the Brute Force technique, to employ sophisticated and effective cryptographic algorithms. As a result, authentication systems are now more vulnerable to attacks and have lost some of their efficacy. Using several authentication factors at once, multi-factor authentication has become a reliable method of cloud security. This makes use of
several tiers of cascaded authentication verifications. The adoption and applicability of various factors for authentication for multi-factor authentication techniques are covered in-depth and methodically in this study. The survey's conclusion relates to developing a distinct authentication factor for multi-factor authentication that doesn't require any extra, specialized gear or software. The procedure of such authentication also makes use of the unique biometric traits of the user in question

3. PROPOSED SYSTEM

The suggested approach is applicable to a variety of fields, including e-health, e-government, and online banking. The protocol is illustrated using the online banking system. putting forth and presenting our authentication method. This protocol consists of four algorithms: The user uses SHA-256 to decrypt the verification code, and the server uses it to verify the user based on the data received. Hybrid one-time passwords employing random OTP SHA-256 bits allow for the encryption and signing of ticket information. The user has to configure two things before starting: the protocol's validity period and the server's authorization. In our project, we employ secure multi-factor authentication based on the usage of image and data encryption.

Verification code

3.1 . REGISTRATION MODULE

A key element of the Hybrid one-time password (OTP) system, the Registration Module is in charge of safely registering customers for the mobile banking app. Users must give some information upon registration, such as account credentials and personal information. To safeguard private information and prevent unwanted access, this module uses strong encryption algorithms. It also creates distinct user profiles and associates them with safe passwords that are used for further authentication procedures.

3.2 SERVER MODULE

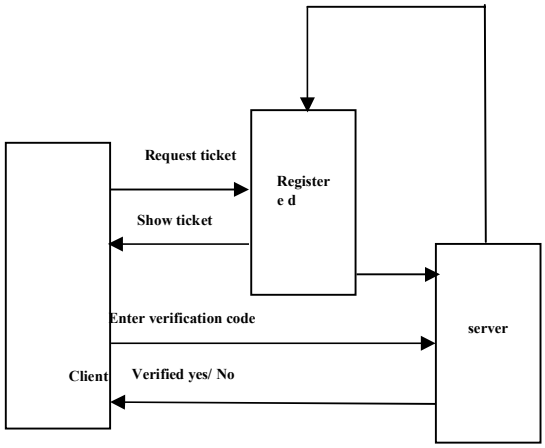
The OTP system's central processing unit, or Server Module, is in charge of overseeing its main features. It increases the overall security of the authentication process by creating and storing one-time passwords using the SHA 256-bit

encryption technique. Additionally, the Server Module coordinates secure data sharing by enabling smooth communication between the client and server components. It is essential to the safe completion of mobile banking transactions since it ensures the secrecy and integrity of the OTPs that are produced.

3.3 CLIENT MODULE

The user interface that allows people to communicate with the mobile banking system is called the Client Module. Users start transactions and authentication procedures with this module. It offers an easy-to-use interface with features that are intuitive, responsive design elements, and clear instructions. In order to generate and verify OTP, the Client Module talks with the Server Module. This keeps the user interface fluid and easy to use while guaranteeing that users can safely access their accounts and complete transactions.

Figure 3. Block Diagram



3.4 OTP VERIFICATION

An essential module that verifies users' authenticity during transactions or login attempts is OTP Verification. This module uses SHA 256- bit encryption for a safe verification method as it compares the OTP that the user enters with the one that the server module generates. When OTP verification is successful, users are able to access the requested functionality. This adds an extra layer of protection by verifying the user's identity and prohibiting unwanted access.

4. RESULT ANALYSIS

algorithm	accuracy
Existing system	75
Proposed system	81

The accuracy rate of the current mobile banking system, as represented by the system in place, is 75%. Although banks frequently promote online banking and provide security guarantees, there are recognized security issues with this approach. Users that conduct mobile banking transactions run the danger of their security being compromised by a variety of threats, such as phishing attempts, botnets, and Trojan horses.

Despite being in place at the transaction level, the present multifactor authentication systems might not completely address the potential weaknesses, leaving room for man-in-the-middle attacks. A suggested approach has been unveiled in response to these security issues, with the goal of improving internet banking's general security. This suggested solution combines SHA-256-bit encryption with a hybrid one-time password technique that uses random OTPs. By operating at both the transaction and authentication levels, this multifactor authentication technique aims to alleviate the shortcomings of current systems. By reducing the dangers connected with mobile banking, this improvement aims to give consumers a safer environment. Based on the data, the suggested method has an accuracy rate of 81%, which is greater than the current system and suggests that the security measures are better. With SHA-256-bit encryption and random one-time passwords (OTPs), the hybrid one-time password technique improves the overall security and dependability of the mobile banking system, as evidenced by this improvement in accuracy. It is imperative to acknowledge that precision in isolation may not provide a whole picture. Therefore, other factors such as adaptability, regulatory compliance, and user experience should also be considered for a comprehensive evaluation of the proposed system.

5. CONCLUSION

Conclusively, the suggested Hybrid OTP technique utilizing SHA 256-bit encryption is a noteworthy advancement in fortifying the security of mobile banking applications. This method provides a strong authentication technique by mitigating the inherent dangers of online transactions, especially in light of emerging cyber threats such as phishing and man- in-the-middle assaults. In order to achieve a balance between increased security and user comfort, user-friendly input and output designs are combined with a focus on authentication at both the transaction and login levels. However, careful consideration of usability, continual observation, and flexibility in response to new security threats are necessary for successful deployment and broad adoption. With its diverse methodology, the Hybrid OTP system is well- positioned to improve the overall reliability and integrity of mobile banking systems in the dynamic field of digital finance.

6. FUTURE WORK

In order to handle new cybersecurity risks, future work in this area should concentrate on the ongoing improvement and modification of the suggested Hybrid one-time password (OTP) system with SHA 256-bit encryption. Research efforts could look into the integration of potent artificial intelligence and machine learning algorithms to proactively detect and counter new attack patterns. Furthermore, the system's resilience would be increased by the creation of adaptive security mechanisms that can react quickly to attacks and vulnerabilities that arise in real time. To remain ahead of increasingly complex cyber dangers, cooperation between researchers, financial institutions, and cybersecurity specialists is crucial

REFERENCES

[1] Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749
[2] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, D
[3] A Biometric Authentication and Authorization Searchable Encryption Scheme for Cloud Environments Nita, S.L. and Mihailescu, M.I. 2022 Cryptology, (6), 8.a
[4] Gupta, Awaysheh, Benson, M., Azab, M., Patwa, F., and Sandhu, R. offer an attribute-based access control system for cloud-enabled industrial smart cars. IEEE Transactions on Intelligent Systems, 17, 4288–4297 (2021).
[5] 14. Trends, dangers, and approaches related to user authentication on mobile devices 2020, 170, 107118; Wang, C.; Wang, Y.; Chen, Y.; Liu, H.; Liu, J. Computer. Netw.
[6] Federico, S., Gabriele, C., Roberto, C., and Nicola, Z.: Multi-factor authentication for online banking survey in real-world settings. Digital. Safety. 2020, 95, 101745
[7] Wang, D., Zhang, X., Zhang, Z., and Wang, P. Understanding the security flaws in multi-factor authentication systems for multi-server configurations. Safe. Computer. 2020, 88,101619

[8] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.
[9] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.
[10] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
[11] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
[12] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.
[13] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.
[14] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756
[15] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar ec.2007
[16] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
[17] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019
[18] Characteristics in ABAC with group hierarchy: reachability analysis IEEE Trans. Reliable Secure Computer. 2022, 20, 841–858, Gupta, M., Sandhu, R., Mawla, T., & Benson, J.
[19] Barkadehi, M.H.; Nilashi, M.; Ibrahim, O.; Fardi, A.Z.; Samad, S. reviewed and categorized the literature on authentication systems in Telemat. Information. 35, 1491–1511 (2018).
[20] Blockchain identity authentication system- based IoT terminal connection service architecture 2020, 160, 411–422. Huang, J.C.; Shu, M.H.; Hsu, B.M.; Hu, C.M. Computer. Communication.
[21] In 2020, Zahid, G., Shafiq, A., Khalid, M., Hafizul, S., Mohammad, M.H., and Giancarlo, F. introduce an improved authentication technique for remote data access and sharing over cloud storage in cyber-physical-social systems. IEEE Access 8, 47144–47160.
[22] 9.Iris Technology: An Overview of Biometric Systems Based on Iris for Personalized Human Identification, Int. Granth aalayah J. Res. 2018, 6, 80–90; M.V.B. Reddy, V. Goutham