IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ALTERNATIVE TO TRADITIONAL CREDENTIAL-BASED AUTHENTICATION

[1]Chandana A T, [2]Nafisa Fathima, [3]Sathela Haswitha, Yeddula Nandini

[1]Student, [2]Student, [3]Student, Student

[1]Computer Science and Engineering,

[1]Presidency University, Bangalore, India

Abstract: User authentication plays a crucial role in maintaining the security of wireless communication technology, given its swift expansion. Passwords are essential to the authentication process. For instance, biometric authentication may be very convenient and safe, but it may also cause privacy issues. Conventional credential-based authentication techniques, including passwords and usernames, have long been the norm for safeguarding private data and protecting digital networks. But the rise of data breaches and the complexity of cyberattacks have brought to light the shortcomings of these traditional strategies. Researchers and practitioners have been investigating substitute authentication techniques that provide improved security, privacy, and usability to address these issues. An overview of the newer alternatives to conventional credential-based authentication is intended to be provided by this abstract. It goes over several creative approaches that make use of cutting-edge ideas and technologies to authenticate users in a way that is both safer and easier to use.

Index Terms - authentication, usernames, passwords, secure authentication, usernames, passwords, secure

I. INTRODUCTION

In 2014, Plagiary reported that 47% of adult American accounts had been compromised. Hackers provide personal information about them. More consumers don't think that passwords can secure their internet accounts anymore because of the issue. Suleyman (2017) claims that some hackers will turn hijacked email accounts into profit by selling them to other people. Today's quickly changing digital world demands secure access to online services and important information, and authentication is essential to attaining this. But as technology develops, conventional authentication techniques like usernames and passwords have shown to be constrained and open to malevolent exploitation by cybercriminals. The hunt for substitute authentication techniques that boost security and improve user experience is therefore highly motivated. The primary disadvantage of conventional credential-based authentication is that passwords are inherently weak. Individuals frequently select predictable or frequently used passwords, leaving them vulnerable to brute force assaults and compromise in significant data breaches. Furthermore, passwords might be misplaced or forgotten, which can be unpleasant for users and require difficult recovery procedures. It is no longer sufficient to protect digital assets and sensitive information alone with passwords. Alternative authentication techniques have been developed in response to these worries, with the goal of improving authentication via cutting-edge ideas and technologies. One such technique is biometrics, which verifies an individual's identity by using their distinct physiological or behavioral traits, such as speech patterns, fingerprints, or facial features. Biometric data offers a high level of security since it is intrinsically hard to copy or falsify. Furthermore, biometric authentication makes it unnecessary for users to memorize complicated passwords, which improves ease and lowers the risk of security breaches involving credentials. Apart from fingerprints and multi-factor authentication, scientists are investigating novel techniques for authentication. For example, contextual authentication evaluates the validity of access requests by considering contextual data like device, location, and behavioral patterns.

Furthermore, behavior-based authentication has been developed because of advances in artificial intelligence and machine learning. In this approach, computers examine user behavior patterns to identify anomalies and possible security risks. It's crucial to remember, though, that there are difficulties with biometric authentication. Careful consideration of privacy issues pertaining to the usage and storage of biometric data is necessary to guarantee user confidence and regulatory compliance. Additionally, variables like sensor quality, ambient circumstances, and the possibility of spoofing attacks affect how accurate and dependable biometric systems are. These factors highlight how crucial it is to put strong security measures in place and to regularly review and update them.

For this study secondary data has been collected. From the website of KSE the monthly stock prices for the sample firms are obtained from Jan 2010 to Dec 2014. And from the website of SBP the data for the macroeconomic variables are collected for the period of five years. The time series monthly data is collected on stock prices for sample firms and relative macroeconomic variables for the period of 5 years. The data collection period ranges from January 2010 to Dec 2014. Monthly prices of KSE -100 Index are taken from yahoo finance.

II. Background Study and Related Work

The process of authenticating a person's credentials to carry out an action is known as authentication. The procedure is finished, and the user will be given access if the credentials match. Typically, in order to access a system service, the user must first provide their password. User authentication, according to Rouse (2014), permits access to network and Internet-connected systems, applications, and resources by allowing human-to machine interactions in operating systems and applications as well as wired and wireless networks. According to Bonneau (2015), who studied the evolution of passwords, the shared operating system included the password in the 1960s. However, the unencrypted password master file breach caused the issue to surface extremely fast. The password began to be saved in hashed form when the 1970s rolled around. With the addition of salting, the hashed password was enhanced in 1979. Since the World Wide Web was launched in the middle of the 1990s, public key cryptography has been used to safeguard passwords through secure sockets layer (SSL) client certificates. Next, two-factor authentication is introduced, and the password is linked to the email. Early in the decade of 2010, smartphone use begins to spread. Free smartphone apps that function as a second component based on the developing time-based-time-pad (TOTP) standard are another driver driving the implementation. The TOTP algorithm uses the current time and a shared secret key to generate a one-time password. As a fallback authentication method, there are further services that involve transmitting codes via short messaging service (SMS). According to Denso (2016), who studied the evolution of passwords, Japan invented the Quick Response (QR) code in 1994. Because of its fast-reading speed, it gets its name from the word "quick response." Barcodes have evolved into QR codes. The evolution is brought about by the fact that barcodes can only contain 20 alphanumeric characters. Masahiro Hara and his development team then worked on the project for a year and a half. The QR code's ability to store 7,000 numerals and finally create the ability to code Kanji characters has made it a big hit. With today's technology, scanning a QR code can assist in redirecting to a website or discount code.

III. Proposed Study

The new system's implementation is the suggested way to improve the login authentication system's security. It will contribute to improving password security in the new system that is being proposed. The system will assist in making sure that the password is not sent through the traffic. To give users more options for logging in, this project uses a QR code as the random key each time they try to log in. Attackers will find it difficult to decode the password using this method because, if the random key is long enough, they will need to create a large rainbow table. In the suggested system, the user enters their username to get their password. A forty-character random key in the form of a QR code will be generated by the server. The random key will then be obtained by the phone scanning the QR code. The random key and hash will then be combined into the password. After extracting the password from the database, the server will hash it using a combination of random keys. The first six characters will be used as the OTP for both of the produced hash values. The login is successful if both matches are found.

IV. METHODOLOGY

PHASE 1: Activity and Cardinality One-to-one, one-to-many, and many-Tomany connectivity are the three fundamental forms of relational connectedness. When at most one instance of entity A is connected to one instance of entity B, this is known as a Oneto-one (1:1) relationship. For instance, "Every employee in the company has a designated office." There is a specific office for each employee, and there is a specific employee for every office. In a one-to-many (1: N) relationship, there is only one instance of entity A for every one of entity B, although there may be zero, one, or many instances of entity B for every one of entity A. A department with a large workforce is an example of a 1: N connection. When there are zero, one, or many instances of entity A for every instance of entity B, and there are zero, one, or many instances of entity A for every instance of entity B, we have a many-to-many (M: N) relationship, also known as non-specificity. The mapping of connected variables is described by a relationship's connectivity.

PHASE 2: ER Notations The way data objects are represented in ER diagrams is not standardized. Every modelling technique has a notation of its own. Although Chen's original notation is frequently used in academic literature and journals, it is rarely used in CASE tools or non-academic publications. Many notations are used nowadays; the most often used ones are IDEFIX, Bachman, and Crow's Foot. Entities are represented as rectangular boxes in all notational systems, and relationships are shown as lines connecting boxes. A unique set of symbols is used by each style to indicate a connection's cardinality. Martin's notation is used throughout this document.

The symbols used for the basic ER constructs are:

- Entities are represented as rectangular boxes in all notational systems, and relationships are shown as lines connecting boxes. A unique set of symbols is used by each style to indicate a connection's cardinality. Martin's notation is used throughout this document.
- One way to depict relationships is as a solid line joining two elements. Above the line is written the relationship's name. Names for relationships ought to be verbs.
- When present, attributes are listed within the entity rectangle. The attributes that serve as identifiers are highlighted. Names for attributes ought to be singular nouns.
- A line that ends in a crow's foot symbolizes the ordinariness of many. The cardinality is one if the crow's foot is not included.
- Putting a circle or a perpendicular bar on the line represents existence.

V. IMPLEMENTATION

The process of turning the theoretical design into a functional system is called implementation. The most important phase in creating a new, successful system and instilling users' faith that it will function properly and efficiently.

VI. FUTURE WORK

Since traditional authentication systems are frequently vulnerable to compromise, many papers advocate for alternate solutions. Nonetheless, the primary causes of this include ambiguous policies, inadequate security measures, and improper infrastructure configuration. To thwart common channel attacks, it is imperative to have multifaceted authentication keys that are generated, dispersed, and kept on several communication channels. Directory services like LDAPs and Active Directory are used to maintain authentication servers. Despite the authentication server having security mechanisms in place, connections to the directory servers are frequently insecure, and front-facing services may not be able to see the database itself. It is possible to construct specific infrastructure needed for the development of novel authentication mechanisms for older systems without completely overhauling the current infrastructure.

VII. CONCLUSION

Although traditional credential-based authentication has been around for a while, it has several drawbacks and difficulties. Security flaws are frequently caused by reused passwords, weak passwords, and forgotten passwords. The hazards connected to conventional authentication techniques are further increased by social engineering assaults and credential theft. Traditional credential-based authentication has considerable disadvantages as well, including user annoyance and password fatigue. People find it difficult to remember complicated passwords across several accounts, which can be frustrating and pose security problems. Users' inconvenience and complexity are increased with the use of two factor authentication (2FA) and regular password changes. Alternative techniques including biometric authentication, multifactor authentication (MFA), and password less authentication have arisen to overcome the drawbacks of conventional authentication. These techniques provide less dependence on passwords, increased security, and ease of use.

While multi-factor authentication (MFA) adds an additional layer of security, biometric authentication uses distinctive physiological or behavioral characteristics to verify an individual's identification. These methods improve security against assaults and address the shortcomings of conventional credential-based authentication. But it's crucial to weigh the benefits and drawbacks of each authentication technique and select the best one for your purposes and the particular security requirements. Maintaining a strong authentication system requires following best practices and remaining current with emerging threats and technologies in authentication. In general, conventional credential-based authentication is still useful, but considering the constantly changing cybersecurity threat landscape, it is critical to use more safe and convenient authentication techniques.

VIII. FIGURES

FIG 1. APP

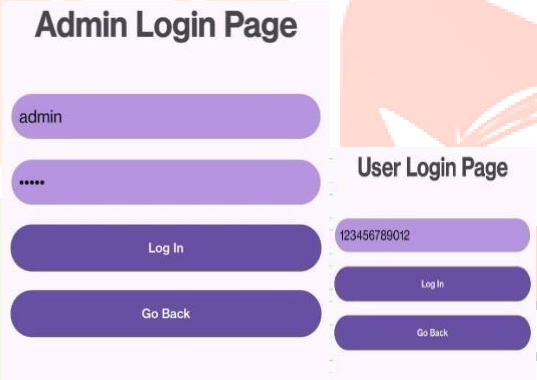

FIG 2. ADMIN AND USER LOGIN PAGE

FIG 3. OTP PAGE

REFERENCES

[1] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. New York: Wiley, 2008 [2] R. G. Rittenhouse, J. A. Chaudry, and M. Lee, "Security in Graphical Authentication," Int. J. Secure. Its Appl., vol. 7, no. 3, pp. 347–356, 2013.

[3] K. I. P. Patil and J. Shimpi, "A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices," Int. J. Innov. Technol. Explor. Eng., vol. 2, no. 4, pp. 155–157, 2013.

[4] A. H. Lashkari, S. Farmand, D. O. Bin Zakaria, and D. R. Saleh, "Shoulder Surfing attack in graphical password authentication," Int. J. Compute. Sci. Inf. Secure., vol. 6, no. 2, p. 10, Dec. 2009.

[5] K. Renaud, "On user involvement in production of images used in visual authentication," J. Vis. Lang. Compute., vol. 20, no. 1, pp. 1–15, Feb. 2009