iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VII **Month of publication:** July 2024

DOI: https://doi.org/10.22214/ijraset.2024.63645

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

Multifactor Authentication: Protecting Privacy in the Digital World

Akshay Nishikant Gawde
Department of Information Technology, Sathaye College, Mumbai, India

Abstract: ***In today's world, digitalization decisively penetrates all the sides of the modern society. One of the key enablers to maintain this process secure is authentication. With the rapid evolution of wireless communication technology, user authentication is essential to ensure the security of wireless communication technology. It assists humans to interact with everything by enabling services that are faster, user-friendly and reliable for authentication. As from conducted surveys, a common user may have multiple online accounts which requires passwords. As an evolution in wireless communication, the user authentication plays an important role. In the process of authentication, passwords plays an important role. Importance of MFA ensures the user's account does not get easily attacked by the attackers and also ensures that the sensitive information of the user remains safe.***

The objective of the system outcome is to enhance the current login authentication system. It provides solutions for making password breaking more difficult as well as convinces users to create passwords that are hard to break. This research delves into the effectiveness of MFA in diverse contexts, including its role in preventing phishing attacks, enhancing security, and adapting to emerging threats. MFA goes beyond conventional password protection, requiring users to authenticate through a combination of knowledge-based factors (Passwords, Pins), possession- based factors(Tokens, Smart-phones), and inherence-based factors(Bio-metrics). This paper explores the concept of MFA, which means combining the various types of authentication factors to enhance user security.

Keywords: Password, 2FA, MFA, OTP, Authentication

I. INTRODUCTION

Due to increasing technology, there is also an increase in the number of smart devices and various electronic gadgets across the globe. In situation where the user's are connected across the globe, the user's data is being transmitted over the network, this is where the authentication comes into picture. Authentication is an activity to authenticate the users credentials that wish to perform the actions on the system. Authentication process is completed when the users credentials is matched with the credentials stored in the system and then the user is granted access. Passwords plays an important role in the process of authentication. In the process of authentication, the user will first enter the password that will be transmitted to the authentication server, to allow the server to grant access to authorized user. MFA is a common and most increasingly used security measure which is been implemented in day-to-day online services which ensure to validate the user's identity to provide access to the system.

Authentication is a fundamental safeguard against any illegal access to any devices or any applications that may require sensitive information regardless it may be offline or online. In earlier days, the only method for authentication while performing transactions was primarily the physical presence; as compared to present days with the advanced technology, the validation is based on the sender identification only. It is important to protect our own account because our credit is priceless. It is hard to trace the attackers in the cyber-world. The secure login system is crucial to ensure the safety online.

From a survey conducted it shows that, the Cam4 data breach that happened in March 2020 approximately exposed 10 billion user records which resulted in stolen credentials in different sectors such as Bank, Health-care, Institutes and many more organizations including Twitter and Facebook.Therefore, this project would like to provide alternative ways to securely log in to a system.

The current MFA methods requires two or more authentication methods from the user. Following are the methods used for authentication:

1) Something that you know. (Password, Pin)
2) Something that you have. (Otp, Tokens)
3) Something that you are. (Fingerprints ,Facial recognition)

II. RESEARCH ELABORATION

A. Objectives

1) The primary objective of multi-factor authentication is to reduce the risk of account takeovers and provide additional security for users and their accounts.
2) Second and most important objective is the implementation of a secure login authentication system by using the concept of 2FA(2 Factor Authentication). By the implementation of 2FA, it would increase the strength of the login system and will help to enhance the authentication process.
3) Generate One-Time-Password that would be in the offline mode.This would help the user to proceed to the authentication process and get access to the system even if there is weak or no connection of Wi-Fi or mobile signal on the users device. e.g: Google Authenticator can be used which implements the concept of TOTP (Time based one-time passwords) that generates new passwords automatically every minute even without internet connection.
4) Ensure login passwords are securely transmitted. Previously, password were just encrypted so it was easily attacked by the attackers to decode the data and retrieve the password.
5) Develop an authentication system that can easily be adapted to use different authentication methods. If one factor is compromised then the attacker still has at least one or more barriers to breach before successfully breaking into the target.
6) Since over 80% of data breaches happen due to weak or stolen passwords, MFA can provide added layers of security necessary to protect users and their data.
7) The goal is to add an extra layer of protection beyond the traditional username and password combination, which can be more susceptible to unauthorized access due to various security threats.
8) MFA reduces the risk of unauthorized entry by adding an extra layer of verification to grant access to the system.

B. Scope

1) *Increased Security:* MFA significantly reduces the risk of unauthorized access, even if passwords are compromised.
2) *Compliance Requirements:* Many regulations and standards (like GDPR, HIPAA) mandate MFA for sensitive data protection.
3) *Increased User Trust:* Implementing MFA can enhance customer trust and confidence in digital services.
4) *Versatility:* MFA can be used across various platforms, including online banking, corporate networks, cloud services, and personal accounts.
5) *User Education and Adoption:* Effective communication and training can facilitate smoother adoption and improve user experience.
6) *Integration with Existing Systems:* Many platforms offer built-in MFA options or easy integration with third-party solutions.
7) *Ease of Adaptability:* Organizations can customize the MFA solutions based on risk levels, user roles, and access.
8) *Future Trends:* Advancements in biometric technology and mobile authentication apps are likely to shape MFA solutions moving forward.

C. Methodology

To understand the impact of digital security awareness, a comprehensive approach was undertaken, including literature reviews, surveys, and case studies. This research aims to identify best practices and strategies for improving awareness of digital security across diverse populations.

1) *Literature Review:* A thorough review of existing methods used for authentication provided insights into the current state of security methods used and the gaps that need to be addressed to enhance user security. The literature review encompassed academic studies, reports, and publications that helped to better understand the functional and non-functional requirements.
2) *Case Studies:* Examining successful implementations of secured login methods that helped in understanding the effective strategies for improving digital awareness for protecting privacy and securing user accounts. These case studies focused on programs that have demonstrated significant improvements in securing the data effectively.

III.DESIGN AND IMPLEMENTATION

A. Types Of Authentication Factors

Key areas to explore could include different types of authentication factors (e.g., biometrics, passwords, tokens), usability considerations, security vulnerabilities, and the impact of MFA on overall system security. We can study the various trends, challenges, and emerging technologies in the field of MFA to provide a comprehensive overview.

Different types of Authentication factors used in this project are as follows:

1) *Passwords:* Passwords are used to secure the online data of a user since early existence of internet. As passwords do not expire for a longer period of time, so the users tend to use the same passwords for longer use which leads to cyber-attacks. The secret pass-phrase traditionally represents a knowledge factor. It requires only a simple input device (at least one button) to authenticate the user. Passwords have been the most significant factor of risk because they are more vulnerable to threats and attacks.
2) *One-Time-Password:* One-time-password (OTP) is a temporary and a unique code which is commonly used for authentication purpose. OTP's are valid for only one time login session and then it becomes invalid. OTP's are valid for short period of time, typically for 30 to 60 seconds which means many of them are time-based.
3) *CAPTCHA:* CAPTCHA stands for (Completely Automated Public Turing Test to tell Computers and Humans Apart). It is a challenging-response technique to identify whether the user is human or not. As it is commonly used on websites to prevent actions like posting spam, creating accounts or purchasing bulk of tickets to avoid automated bots to do so.
4) *Distorted Text:* It is the most common type of CAPTCHA which is used to display sequence of distorted letters and numbers, that users have to type correctly to get identified.
5) *Number CAPTCHA:* It is the second common type of CAPTCHA, which is also used to identify the user by challenging them to solve numerical problems which are easy to understand and solve by the humans and difficult to pass for an automated bots as the mathematical expression refreshes automatically after each attempt.
6) *Facial Recognition:* Facial Recognition is a type of biometric technology which is used to verify the user by the facial features which is being compared and analyses the patterns. Using this technology, it ensured numerous benefits in terms of security, convenience and efficiency.This is mostly used in Banking sectors to verify the user details and KYC.

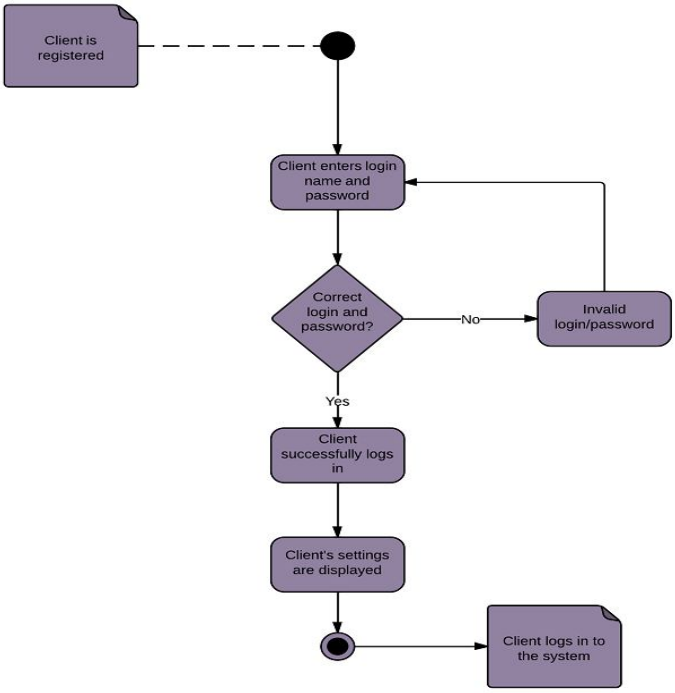


Fig.1:Process of Authentication

a) The user visits the login page and enters their credentials to gain access to their account.
b) During authentication, the password entered by the user will be transmitted to the server in order to allow the server to grant access to the authorized user.
c) The user needs to solve a CAPTCHA after entering the credentials.The user gets access only if the credentials are matched with the credentials present in the database or else he will not be allowed to access the system.
d) The user receives an OTP or a confirmation mail which informs the user that someone is trying to login to their account.
e) The user gets access to their account when the credentials are confirmed as correct.

IV. RESULTS AND DISCUSSIONS

A. Results

Fig.2: The user interacts with the system

The user interacts with the system and has options to Register and Login to the system.

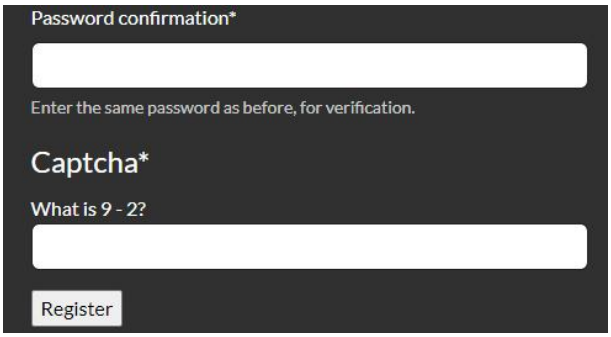


Fig.3: Implementing Number CAPTCHA

After entering the credentials the user needs to solve the number CAPTCHA to get registered in the system.

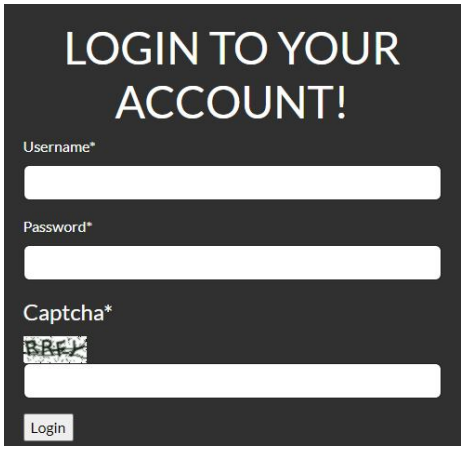


Fig.4: Implementing Distorted/Text CAPTCHA

The user needs to enter the Username and Password and solve the Distorted CAPTCHA to get access to the users system.

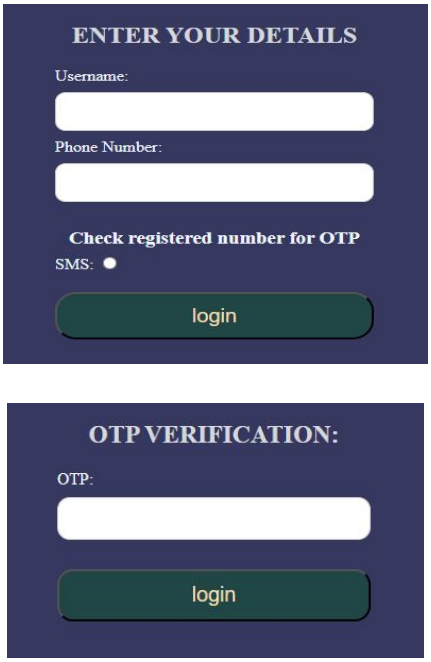


Fig.5: Implementing OTP Authentication

The user enters the credentials and then he will receive OTP on the registered phone number and after entering the correct OTP the user gets access to the system.

B. Benefits of Multiple Factor Authentication

1) *Consumer Identity:* MFA is an important tool for protecting consumer data from identity theft. By implementing this measure, the security of the traditional username and password login is supplemented by an additional layer of protection.
2) *Compliance:* Implementing multi-factor authentication can be a key requirement when it comes to complying with certain industry regulations. For example, PCI-DSS requires MFA to be implemented in certain situations to prevent unauthorized users from accessing systems. So, even when application updates lead to unknown and unattended consequences, MFA compliance ensures that it remains virtually non intrusive.
3) *Easy Implementation:* Multiple factor authentication by its very nature, is non invasive. It does not affect the rest of the virtual space of an organization or institution. To add, its intuitive user experience allows it to be picked up by the consumer with almost little to no effort.
4) *Security:* MFA can help block such users and even report potential threats. The IT department immediately gets notified. They can take strict actions to block such users.The rise in password thefts through phishing, key logging, and pharming has raised many concerns for organizations across the globe, especially on an open network. All these concerns can be laid to rest through the implementation of MFA.
5) *MFA Takes Away Password Risks:* Password risks can be extremely common. If cyber-criminals were to find your duplicate passwords, it makes it easier for them to gain access to multiple of your accounts. By adding MFA, the cyber-criminal will not be able to access your accounts without first authenticating who they are.

C. Challenges faced in Multiple Factor Authentication

1) *Lack of user Education:* Users may use the same passwords for their email and application login, not understanding the risk this can pose in the implementation of a MFA system.
2) *Phishing Attacks:* Phishing attacks can result in users entering their login credentials into illegitimate online forms. This enables attackers to hack into their email accounts and retrieve codes sent by an MFA system.
3) *Lack of Regular Updates:* MFA system providers continuously work to improve the security of their products—for example, by strengthening authentication protocols and enhancing encryption algorithms. Not updating the MFA system means missing out on necessary security improvements.

4) *Implementation and Maintenance COSTS:* Implementing and maintaining MFA can be expensive, especially for small businesses or organizations. It may require hardware and software upgrades, additional training for employees, and ongoing maintenance costs.
5) *User Resistance:* Some users may find MFA cumbersome and time-consuming, especially when using multiple devices to authenticate. This may discourage them from using it, which could compromise the security of their accounts.
6) *False Sense of Security:* While MFA is more secure than single- factor authentication, it is not foolproof. Hackers can still find ways to bypass MFA, such as through social engineering attacks or by intercepting SMS based one-time codes.

V. CONCLUSIONS

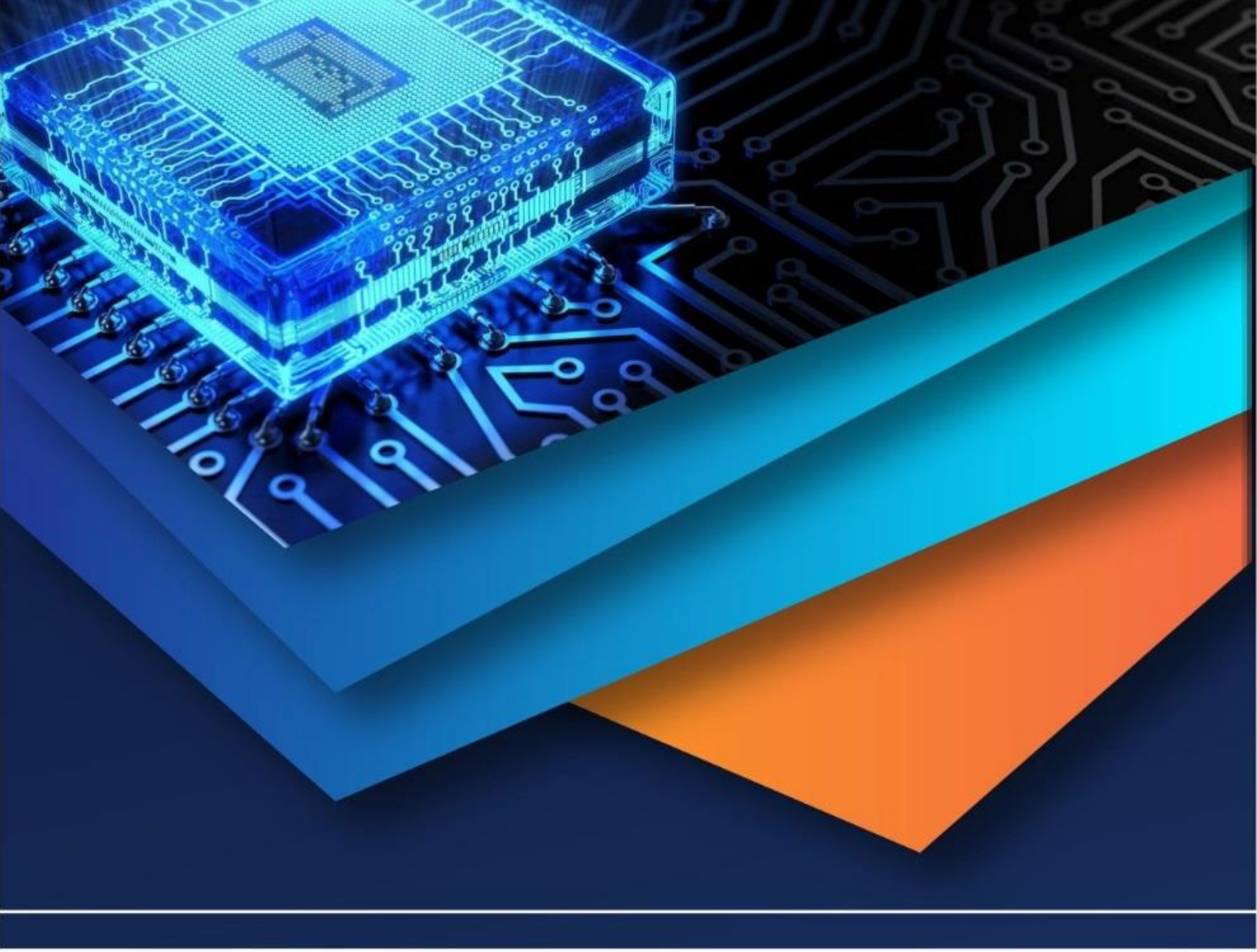
This paper is to help understand the concept of Multi-Factor Authentication (MFA) and spread awareness about its benefits. Multi-factor authentication being used in one form or another is much more secure than only using a username and password. The necessity of utilizing MFA cannot be overstated, as it will increase the security of any system. With users becoming increasingly aware of security issues and the importance of protecting their online data, their first step in increasing the security of their accounts should be to enable multi-factor authentication. Moreover, giving the fact of MFA benefit, where it wins over 2FA by adding third layer of security in addition to user's credentials and PIN. The first step is for companies to implement MFA options for their users. User's will be able to login to several common services and applications by checking credentials one time and leveraging Multi-Factor Authentication. The implementation of the authentication systems fulfilled the goal of implementing a system that can easily be adapted to use different authentication methods. The analysis of the field of continuous authentication showed that it constitutes various factors for this type of authentication. One of the most promising directions in MFA is behavior-based biometrics providing entirely new ways of authenticating the users. This work provided a systematic overview of the state in both technical and usability issues, as well as the major challenges in currently available MFA systems. The implementation of multi-factor authentication methods should only increase year by year allowing it to become more familiar to the users.

VI. ACKNOWLEDGMENT

I would like to express my heartfelt gratitude to Mr. Chayan Bhattacharjee for his valuable guidance and support throughout the development of this research paper. His insights and expertise have helped define the scope and quality of this project. I am also grateful to Mrs. Sumedha Barve, the head of the IT Department, for her continuous support and encouragement. Her leadership and vision provided a solid foundation for this research, allowing me to explore and contribute to this interesting topic. Thank you both for your mentoring and believing in this idea.

REFERENCES

[1] International Journal of Computer Science and Information Technology Research ,Authors: Norah Alyousif, Sultan Alhabis Research Publish Journal (https://www.researchpublish.com/papers/the-necessity- of-multi-factor-authentication)
[2] Multi-Factor Authentication: A Survey, Author: Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey AndreevResearchGate (https://www.researchgate.net/publication/322288752_Multi- Factor_Authentication_A_Survey)
[3] Best Practice in Multi-Factor Authentication, Authors: Joseph Williamson, Kevin CurranResearchGate (https://www.researchgate.net/publication/351852137_Best_Practice_in_Multi_factor_Authentication)
[4] Multi-Factor Authentication, Authors: Emin Huseynov, Jean-Marc SeigneurScienceDirect (https://www.sciencedirect.com/topics/computer-science/multifactor- authentication)
[5] Privacy preserving multi-factor authentication with biometrics, Authors:Shimon Modi, Matthew Young, Anna Cinzia Squicciarini, Abhilasha Bhargav Spantzel ResearchGate:(https://www.researchgate.net/publication/220065411_Privacy_preserving_multi-factor_authentication_with_biometrics)
[6] Secure Login System for Online Transaction Using Two Layer Authentication Protocol, Author:Somnath Sinha ,Research-gate(https://www.researchgate.net/publication/345384866_Secure_Login_System_for_Online_Transaction_Using_Two_Layer_Authentication_Protocol)
[7] Working of 2FA authentication:(https://www.merchantfraudjournal.com/two-factor-authentication-work/)
[8] An Innovative Multi-Factor Authentication Approach, Author:Peter Voege, IEEE(https://ieeexplore.ieee.org/document/9851710)
[9] A Comprehensive Study on Authentication Systems, Authors:Anagha Chaudhari, Ashish Pawar, Adesh Pawar, Ajay Pawar, Ganesh Pawar IEEE(https://ieeexplore.ieee.org/document/10392029)
[10] Multi-factor Authentication as a Service, Authors:Yogendra Shah; Vinod Choyi; Andreas U. Schmidt; Lakshmi Subramanian, IEEE(https://ieeexplore.ieee.org/document/7130879)
[11] Secure login authentication system, Author:CHOW WEN CHAI (http://eprints.utar.edu.my/2855/1/CS-2018-1405547-1.pdf)
[12] Secure login authentication system using captcha based graphical password technique, Authors:Mr. Ganesh Satkar, Prof. Santosh Biradar (https://www.irjmets.com/uploadedfiles/paper/issue_3_march_2022/19657/final/fin_irjmets1646895926.pdf)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY