International Journal For Technological Research In Engineering
Volume 9, Issue 10, June-2022 *ISSN (Online): 2347 - 4718*

REVIEW ON AUTHENTICATION CONCEPT AND TECHNIQUES

Jay Prakash Kumar[1], Md. Saqib Anwar[2]
[1]M.Tech Scholar, [2]Assistant Professor
Department of Computer Science and Engineering
K. K. University Nalanda (Bihar)

Abstract: Authentication is the process of identifying individual users in order to give them access to some system, network, or device. Authentication often works with user credentials like usernames and passwords. It can also use other authentication technologies like biometrics or authentication apps to identify those user identities. Business logic and risk profiles will vary for different companies, so authentication methods may also vary. Authentication is a way to keep your network safe by making sure only those who are allowed on it gain access. This usually involves some form of verification and authorization, such as a password or questioning the user. This paper reviews the concept of Authentication and various techniques available in authentication.

Keywords: User Authentication, User Validation, Hacking, Data Access

1. INTRODUCTION

To stop cyber-attacks, you need to identify unauthorized users. User authentication is when your web application recognizes the user and grants them access to the application. [1]
User authentication is the process of ensuring that only authorized users access your device or network. This procedure can be a login with a personalized password, where an application requests authorized access to it. If the authentication fails, then it means that the user lacks the proper login rights to the network. [1]

User authentication is unaffected by a potential intrusion detection system. The hacker would need to go above and beyond in order to gain access to the network. To protect from cyber threats, use user authentication. Attackers are only effective when they get into the network. The barricade leaves them locked out and unable to disrupt the network as long as it’s strong.

When entering information for user authentication, the computer will either approve or decline your request. When the request is declined, it could be because you have entered incorrect information or forgotten your password.[1]

Fig 1. User Authentication

To access your account, you must provide a form of ID and username. These will confirm the user's identity to the set system which will then grant access. [2]

Authentication is in charge of verifying that someone is who they say they are, whereas authorization defines what type of access a user has after they log in. While authentication and authorization often get used interchangeably, the two terms work together to create a secure login process. It's very easy - just input your credentials on the website login form, and the information will be sent to the authentication server for verification. [2]

If you can't log in, the system will ask you to reenter your credentials and try again. After several unsuccessful attempts, a flag or password reset is required. [2]

2. IMPORTANCE OF AUTHENTICATION

Weak passwords are the leading cause of data loss. There is no easy solution to the problem of password security. Disabling authentication can cause people to lose access to their computer systems and networks, which is dangerous for organizations. Using the right authentication method enables companies to keep their network safe. [3]

Strict authentication of a person seeking access to a building will keep the wrong people out and need an authorized person to enter. This is done by confirming that the person seeking who is requesting entry has clearance, or authority. Authentication is confirmed using an identification card, password, fingerprint, or iris scan. [3]

We use email addresses and passwords to digitally identify ourselves when we perform an action on the Internet or make a purchase. The problem is that a password doesn't authenticate a person; it only authorizes a device, which can be accessed by anyone if they know the person's User ID and password. [4]

Passwords have become too vulnerable to theft, causing a significant crisis in the realm of data security. There are several different forms of user authentication, but the first step is understanding how and why passwords are ineffective. A user authentication system restricts unauthorized users from accessing sensitive information. For instance, User A won't be able to see private data of User B. [4]

If your system is not secure and safeguags are not in place, data breaches can occur- for example, Equifax and Adobe were two companies that were victims of these circumstances. Yahoo, Equifax, and any other organization without a secure authentication process is at risk of a data breach. [4]

3. USER AUTHENTICATION TECHNIQUES

As a result of evolving cyberattacks, security teams are facing plenty of authentication-related challenges. This is why companies are starting to implement more sophisticated incident response strategies, using authentication as part of the process. The list below reviews some common authentication methods used to secure modern systems that you may be familiar with. [5]

- Password-based authentication: To protect your account you need strong passwords with a mixture of letters, numbers and special characters. One simple way to create strong passwords is by following a passphrase pattern. Many people do not use strong passwords or are prone to phishing attacks. Around 54% of users only have one password, which is very unsafe. Many people find it easier to use simple passwords instead of creating a more complicated password, because the latter is more difficult to remember. Passwords are flawed in protection and can't protect online information. The hacker uses all combinations until one guess succeeds. [5]

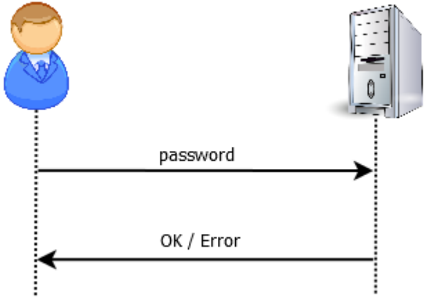

Fig 2. Password Authentication

- Multi-factor authentication: MFA can be done on a smartphone, fingerprint scanning or other methods. The downside is it takes two steps to log in and confirm the account. Additional security measures, such as multifactor authentications, are a good defense against account hacks. Unfortunately, MFA has its own drawbacks. You might lose your phone or SIM and forget your code to login. [5]

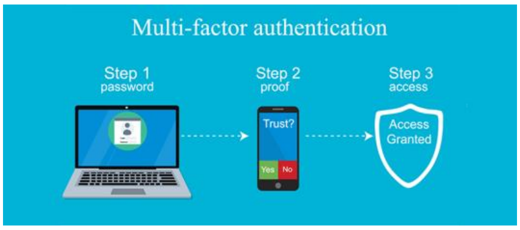

Fig 3. MFA Concept

- Certificate-based authentication: Certificate-based authentication certificates identify devices, users or machines. These certificates are digital documents that copy the idea of a driver's license or passport. Digital certificates are granted when a user has completed authentication and a public key is proven to belong only to them. Their certification authority digitally signs the certificate as valid. When you send a request to a server, it uses cryptography to verify that you are the owner of your digital certificate. [6]

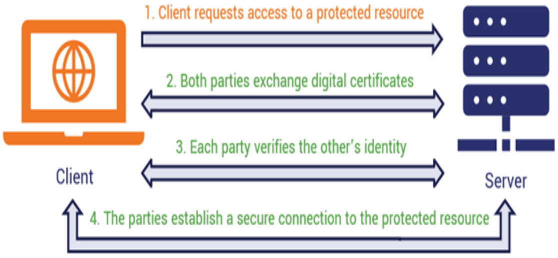
1. Client requests access to a protected resource
2. Both parties exchange digital certificates
3. Each party verifies the other's identity
4. The parties establish a secure connection to the protected resource
Client
Server

Fig 4. Certificate Based Authentication

- Biometric authentication: The Different Ways Your Body Can Be Used as A Password. Biometrics is a security process that relies on unique biological characteristics of an individual. Biometric authentication technology is increasingly adopted because it can achieve a high level of security without creating friction for users. Common biometric authentication methods include facial, fingerprinting, voice recognition, and hand geometry. [6]

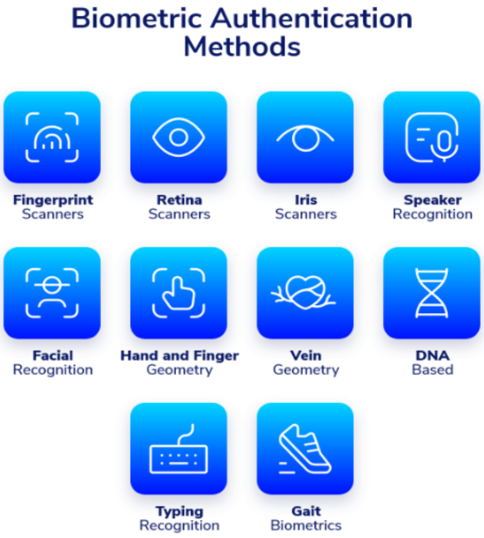

Fig 5. Biometeric Authentication

- Face recognition uses faces stored in databases to authenticate someone. If a person tries to access it from an angle that matches your database, then they are authenticated. When different people look similar (like relatives), then facial recognition could be inconclusive. To prevent people from spoofing their facial recognition, ID R&D’s passive facial liveness is implemented to stop spoofers. [7]

- Some newer fingerprint scanners can assess vascular patterns within a person’s fingers. The popularity of fingerprint scanners can be contributed to the Apple iPhone.[7]
- Speaker recognition technology uses speech patterns to identify an individual. They use words that are standardized in a voice protected device for access. [8]
- Eye scanners fetch data from a person’s unique iris patterns. Eye-based authentication can suffer inaccuracies if a person wears contact lenses or glasses. However, iris scanners are fast and easy to use. [8]
- Token-based authentication: Token-based technologies are becoming a common way to authenticate. A unique encrypted string of random characters is created by the sensor, which can be used to bypass the need for user credentials. One use case includes RESTful APIs - frameworks and clients that use token-based authentication. [9]

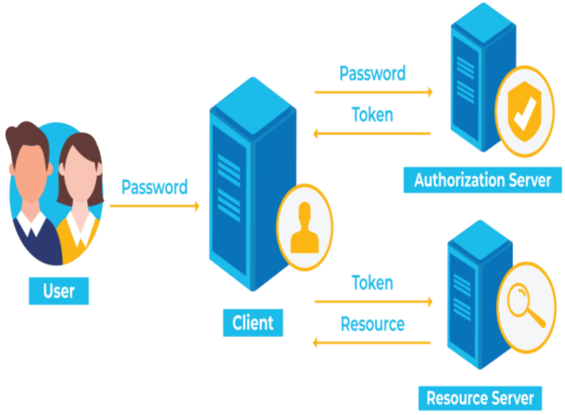

Fig 6. Token Based Authentication

4. SECURING SYSTEMS

Some of the tips by which you can secure your system are as follows, [9]

- Activating multifactor authentication.
- Set up multifactor authentication to reduce the risk of compromising login credentials by adding more layers of security.
- Cybercriminals assume that many users re-use passwords, so make sure you don't.
- It is essential that you generate strong, hard to break passwords in order to protect yourself from hackers. This can best be done by using a password manager. [9]
- Make sure you check if any of your accounts have been in a data breach, and change your passwords for the services the breach is associated with.
- Always use VPNs or mobile access points when connecting to a private service from public WiFi. [10]
- Do not use personal information such as your date of birth or your high school to reset your password.
- To ensure privacy while working in public places, be aware of your surroundings and make sure there is nobody looking over your shoulder.
- Always make use of screen privacy filters to prevent snooping. [10]
- Don't let your devices out of your sight when in public spaces.

5. CONCLUSION

Authentication and user experience are always changing. Businesses should move past passwords to enhance the data. Biometrics technology eliminates the need to remember long and complex passwords, so by having a more secure authentication process, businesses will be able to prevent huge data breaches.

REFERENCES

[1] H. Kim, D. Lee and J. Ryou, "User Authentication Method using FIDO based Password Management for Smart Energy Environment," 2020 International Conference on Data Mining Workshops (ICDMW), 2020, pp. 707-710.

[2] J. Yang, H. Hou, H. Li and Q. Zhu, "User Fast Authentication Method Based on Microservices," 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA), 2021, pp. 93-98.

[3] A. Huang, S. Gao and A. Nathan, "A User Authentication Enabled Piezoelectric Force Touch System for the Internet of Things," 2020 IEEE International Conference on Flexible and Printable Sensors and Systems (FLEPS), 2020, pp. 1-4.

[4] X. Bultel et al. "Security analysis and psychological study of authentication methods with PIN codes" 2018 12th International Conference on Research Challenges in Information Science (RCIS) pp. 1-11 2018.

[5] D. K. Anguiano Cervantes Ghouri Mohammad Saaduddin Y. Li and M. Xie "Comparison between fingerprint and behavioral biometric authentication using 2D and 3D gestures" 2016 IEEE Conference on Communications and Network Security (CNS) pp. 372-373 2016.

[6] S. Kang J. Lee C. Kim and H. Yoo "B-Face: 0.2 MW CNN-Based Face Recognition Processor with Face Alignment for Mobile User Identification" 2018 IEEE Symposium on VLSI Circuits pp. 137-138 2018.

[7] Q. Zhang H. Li Z. Sun and T. Tan "Deep Feature Fusion for Iris and Periocular Biometrics on Mobile Devices" IEEE Transactions on Information Forensics and Security vol. 13 no. 11 pp. 2897-2912 Nov. 2018.

[8] D. El Zein and A. Kalakech "Feature Selection for Android Keystroke Dynamics" 2018 International Arab Conference on Information Technology (ACIT) pp. 1-6 2018.

[9] K. Tse and K. Hung "Behavioral Biometrics Scheme with Keystroke and Swipe Dynamics for User

Authentication on Mobile Platform" 2019 IEEE 9th Symposium on Computer Applications &amp; Industrial Electronics (ISCAIE) pp. 125-130 2019.

[10] J. Park C. Nam J. Lee and D. R. Shin "Analysis of Task Success Rate for Classifying 2D-Touch and 3D-Touch through Threshold" 2019 21st International Conference on Advanced Communication Technology (ICACT) pp. 334-338 2019.