IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115138

Password Authentication Methods Using Various Techniques

Victoria A. Mittapelli[1], P.T. Tandekar[2], S.K Purve[3]

Student, Computer Science & Engineering, Shri Sai Engineering & Technology, Bhadrawati, Chandrapur, M.S, India[1]

Assistant Professor, Computer Science & Engineering, Shri Sai Engineering & Technology, Bhadrawati, Chandrapur, M.S, India[2]

Assistant Professor, Computer Science & Engineering, Shri Sai Engineering & Technology, Bhadrawati, Chandrapur, M.S, India[3]

Abstract: Authentication enables organizations to keep their networks secure by permitting only authenticated user or processes to gain access to their protected resources. this may include computer systems, networks, databases, websites and other network-based applications or services. With the rise in cyber- crime, security threats related to logins & accesses have become a major concern. Also, the use of single security authentication is not sufficient enough to keep you protected from cyber threats. Hence to increase the security level we have Different types of password authentication that will make sure that only the authorized person will have access to the system or data. It contains three-level- logins having three different kinds of passwords systems for ensuring adequate security.

keywords: Authentication, Authentication Techniques, Information system, Security.

1. INTRODUCTION

Authentication system that validates user for accessing the system only when they have input correct password. This involves different levels of user authentication. there are varieties of password system available, many of which have failed due to bot attacks while few have sustained it but to a limit. In short, almost all the password available today can be broken to limit. Hence In this paper we discuss about the various types of authentication system to provide security to the user. Cybercriminals can gain access to a system and steal information when user authentication is not secure. The data breaches companies like Adobe, Equifax, and yahoo faced are examples fail to secure their user authentication. when it comes to authentication and security, there is vast ocean of different authentication options to choose from. Before adopting or choosing any of the authentication methods for our organization employee's or end-user, we should be aware of a few key factors that will help us to choose the most appropriate authentication. security capability of that authentication methods and usability interface.

2. AUTHENTICATION TECHNIQUES

A diverse range of authentication methods have been developed in-recent years. Including two -factor authentication, biometric CAPTCHAs, and many more. Here is a list of the most common password authentication methods.

2.1 STANDARD PASSWORD AUTHENTICATION

This is the most basic form of authentication that everyone will be familiar with. standard password authentication involves a user entering their username accompanied by a secret code passphrase that allows them to gain access to a network, account or application. To reduce the risk of password being compromised, users should choose password with a combination of both letters (uppercase or lowercase), numbers and symbols. A secure password manager or password management software can help with this, storing our passwords under single master password for optimal security

2.2 TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication, or a form of multi-factor authentication, builds on the top of passwords to create a more robust security solution. Two-factor authentication requires authenticate via something we know and something we have. A password serves as "something you know", and the possession of a specific physical object such as a smartphone serves as "something we have", ATMs were an early system to use two-factor authentication because they require both insertion of a debit card and a PIN. Also, it notifies in our devices with push notification or SMS code, or a biometric like,

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115138

finger-print or facial (face ID) or (voice ID) reorganization. Two factor authentication is great option for MSPs and other businesses because it adds an additional layer.

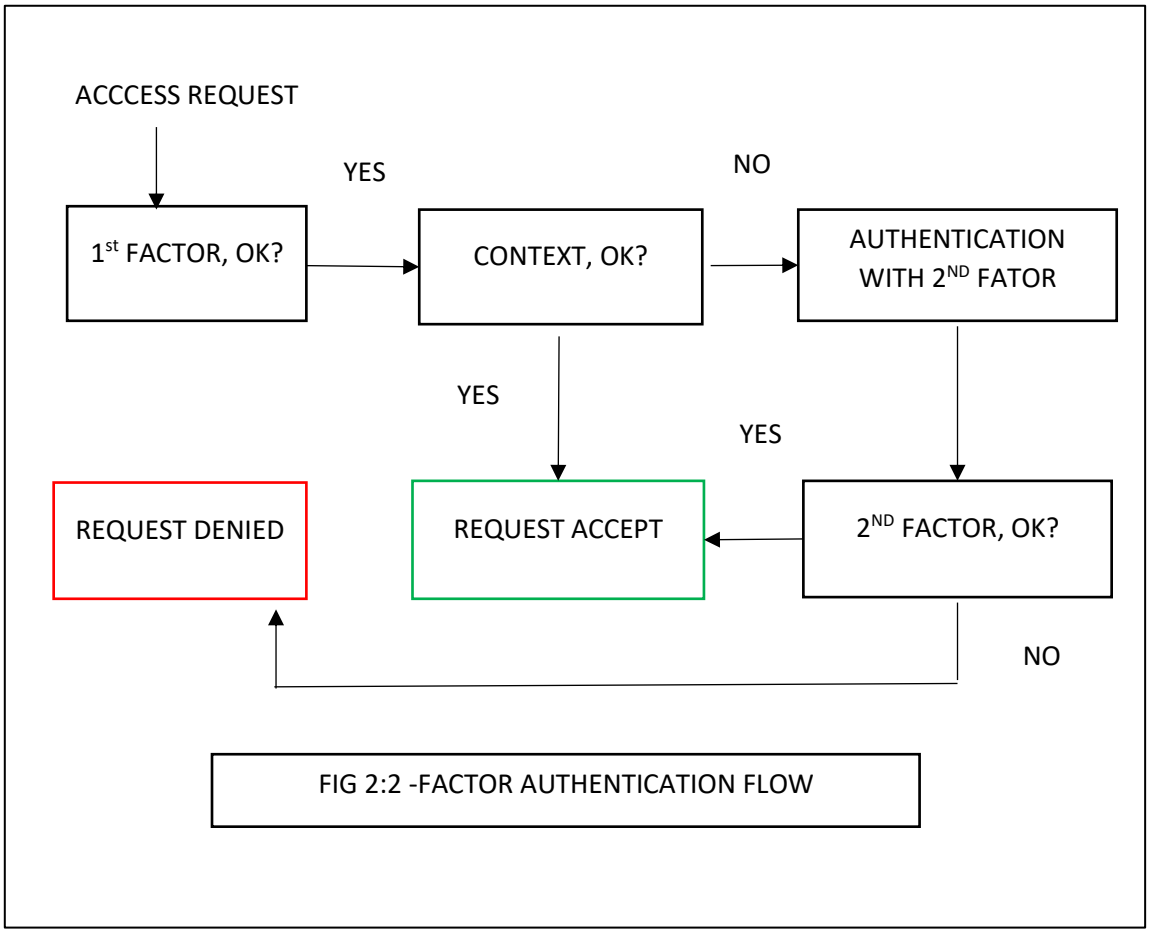

FIG 2:2 -FACTOR AUTHENTICATION FLOW

2.3 BIOMATRIC AUTHENTICATION

Biometric authentication involves using some part of user physical makeup to authenticate user. this could be fingerprint, and iris scan and retina, or some other physical characteristic. A single characteristic or multiple characteristics could be use. This is a highly secure form of authentication because no two individuals will have the same physical characteristics biometric authentication is an effective way of knowing precisely who is login into the system. It doesn't require user to have a card, dongle, or cell phone to hand. They don't even necessarily need to remember their password.

2.4 COMPUTER RECOGANISATION AUTHENTICATION

Computer recognition is a password authentication method that verifies a user's legitimacy by checking that they are on a particular device. These systems install a small software plug-in on the user's device the first time they successfully login. This plug-in contains a cryptographic device marker. When the user next logs in, the marker is checked to make sure they are on the, trusted device's

This system is invisible to the user and doesn't require any additional authentication actions from them. They simply enter username and password as usual, and verification happens automatically. The disadvantage of this authentication method is that it can be cumbersome when users switch devices. To maintain a high level of security, computer recognition authentication systems must enable logins from new devices using other forms of verification (i.e., two-factor authentication with a code delivered via SMS).

2.5 TOKEN AUTHENTICATION

If you prefer not to relay on mobile phones, you might instead use a token authentication system. Token systems use a purpose-built a physical device to deliver two factor authentication. This could be a dongle that is inserted into user device's USB port, or paraphs a smart card with radio frequency identification or near-field communication chip to keep

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115138

a token system secure, it is crucial that is user ensure that user physical authentication device (i.e., dongle or smart card) does not fall into wrong hands.

Token-based system are generally more expensive than other password authentication methods because they require user to purchase purpose-built hardware for each of user. They are however, very secure and most cost-effective options are entering the market as time goes on.

Token-base authentication has following types:

Connected tokens, contactless tokens, disconnected tokens, software token, JSON WEB TOKEN (JWT).

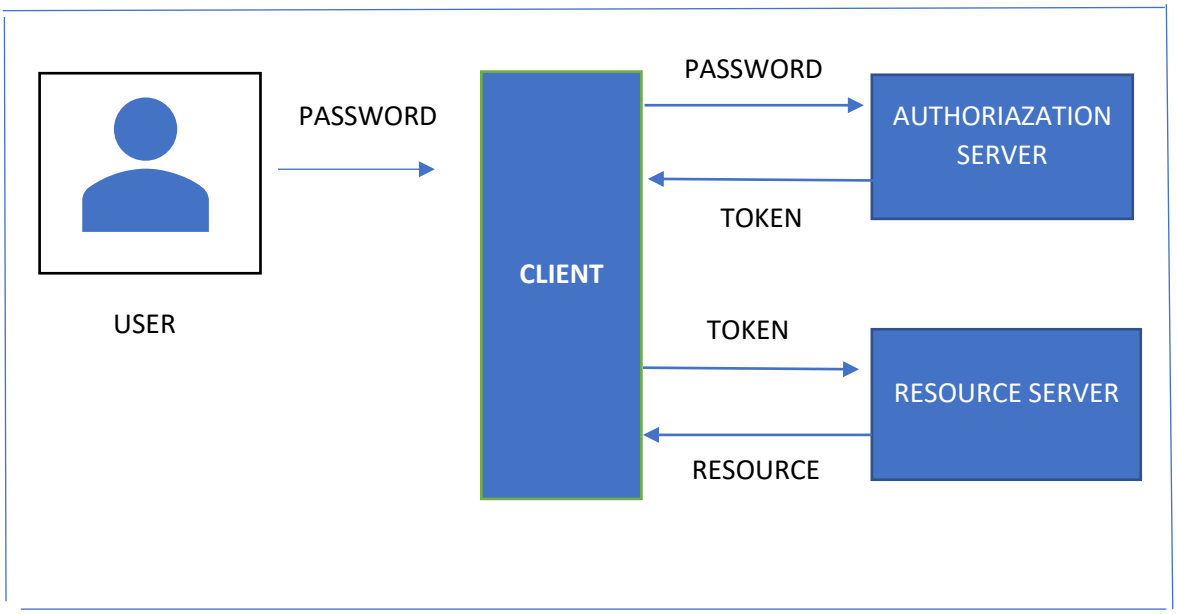

FIG 2.5.1: TOKEN BASED AUTHENTIATION IN WEB API

2.6 CAPTCHAS

CAPTCHAS do not focus on verifying a particular user, as the other methods listed in above do. Instead, CAPTCHAS aim to determine whether a user a human, to prevent computer-driven attempts to break into accounts such as brute force attack. The CAPTCHAS system displays a distorted image of letters and numbers, or pictures, and asks the user to type in what they see. Because computers and bots struggle to identify these distortions correctly, CAPTCHA's enhance security by creating an additional barrier to automated hacking system.

These systems can, however, still cause problems-individuals with disabilities, such as blindness, may not be able to pass a CAPATCHA's test. Even none-disabled individuals sometimes have trouble with CAPTCHAS, which can cause frustration and delays.

CAPTCHAS helps protect you from spam and password decryption by asking you to complete a simple test proves user are human and not a computer trying to break into a password protected account.

3.CONCLUSION

Authentication is proper validation and rights management of the user for accessing the resources of any information system and the most critical element in the field of information security. In this paper authentication methods and techniques are currently available in sufficiently but each has its own profits and loss. That provides a solution to proper authentication and flexibility of offering different authentication options. In this paper we try to cover some of these techniques. To achieve proper sort to authentication with sure mediums.

4.ACKNOWLEDGEMENT

I would like to thankful to the department of computer science & Engineering for providing guidance, useful and practical suggestions, technical support for research environment to accomplish this work.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022
DOI: 10.17148/IJARCCE.2022.115138

5.REFERENCES

1) L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in ElectronicSoc., 2007
2) "Authentication Methods and Techniques", Christopher Mallow
3) L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003
4) M. Manjunath, K. Ishthaq Ahamed and Suchithra (2013): Security Implementation of 3-Level Security System Using Image Based Authentication. Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com Volume 2, Issue 2, March – April 2013
5) A. A. Hassan (2005): Database security and auditing, protecting data integrity and accessibility. 1st edition, course technology
6) A. T. Akinwale and F. T. Ibharalu (2009): Password authentication scheme with secured log in interface. Annals. Computer Science series 7th tome 2nd Fasc.
7) Akazue M. 1 and Efozia, N. F. (2010): A Review of Biometric Technique for Securing Corporate Stored Data