Proceedings of the International Conference on Sustainable Computing and Data Communication Systems (ICSCDS-2022)
IEEE Xplore Part Number: CFP22AZ5-ART; ISBN: 978-1-6654-7884-7

A Comprehensive Study on Passwordless Authentication

Viral Parmar[#], Harshal A. Sanghvi*, Riki H Patel**, Abhijit S. Pandya [$]
School of Technology, Pandit Deendayal Energy University, Gandhinagar, Gujarat, India

*,**,[$]Deparment of CEECS, Florida Atlantic Universisty, Boca Raton, Florida, USA

[#]viralparmar93@outlook.com, *hsanghvi2020@fau.edu, **rikipatel26@gmail.com , [$]pandya@fau.edu

2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) | 978-1-6654-7884-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICSCDS53736.2022.9760934

***Abstract*— In the technology today, user-based authentication and password are now widely used in all information systems and services. Most of the university also uses this type of authentication method for many services, but the password is in danger. By providing a password-protected verification system for the most usable and secure organization. In the old days, the password was used as the best authentication system to prevent unauthorized access. Now the technology in the authentication system is growing day by day so that the password is changed to be more secure. However, the vulnerability of this traditional system has prompted the industry and researchers to find a new alternative where there is no threat such as theft, hacking and cracking passwords. This study discusses in more detail the key strategies for verifying the authenticity of a password in detail and sets out an attempt to explain details and process of each technology. The paper consists of an extensive review of the research conducted in past several years and this research study has presented a review of recent research works which are mainly conducted for improvising the security with the end to end encryption process.**

Keywords— Traditional Authentication, Password less Authentication, Emerging Authentication, Biometrics, Web Security

Introduction

In the world today, we have been substituting passwords with other methods such as end user authentication but none of the methods have been proven reliable in terms of security [1,2]. In the rapid moving updates in technology, the major trend is moving away from the password-based authentication and implementing secured connection which is based on asymmetric cryptography [1]. Recent studies [1,3] have been more focusing on the FIDO2 kings' layer of user authentication. There are various complex distributed systems with the increasing number of users which thrives towards the security challenges resulting in cyber threats [4,5]. As discussed in [6] knowledge-based authentication is the most common method been used. There are many pros in using this authentication method such as it is user friendly, economical, and straightforward to use. The outcome of the survey as discussed in [7] gave the statistics, there were 76% of respondents using the cell phone devices who saves the password in their personal notes which quite often leads to the password been forgotten or stolen. Out of 76%, 33% users require multiple attempts to login to the device as they forget the password quite often. Sixty percent users out of 76% as discussed, showed a trend of resetting the password very often. In 1960, methods like password-based authentication were utilized as the prime authentication method to control access to the mainframe systems [8]. The methods discussed in [9,10] shows the limitations of password-less authentication. As proposed by Stajano [11,12] for replacing password with hardware token, there are various design perspectives associated with U2F and FIDO2.

Figure 1 shows the Access Control Authentication Methods. It shows the wide range of methods available such as Pin Code Authentication, AI powered Biometric Identification, Facial Recognition, NFC Based Authentication, RFID, and Fingerprint Recognition Methods. As identity identification is important for the access these days physically in the similar way identity on the web is also important.

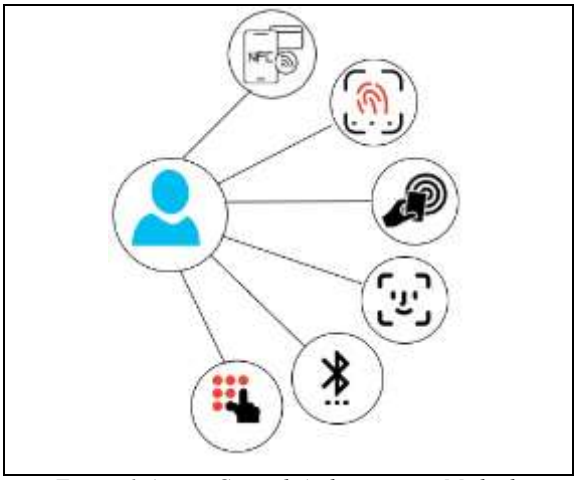

Figure 1 Access Control Authentication Methods

Based on challenge-response protocol, public key cryptography approaches mutual authentication between Pico and Verifier which looks towards the user's privacy. There were various browsers [13] such as Chrome, Firefox, Edge as well as Safari which already deployed Web Authentication. There were multiple websites which supported Web Authentication [14-18]. Storage Instances like Dropbox, Azure, Google Cloud also offered FIDO2-based authentication [19-21]. Usually for the non-browser clients, FIDO2 libraries and tutorials played a supporting role [22-24]. In an open-source environment, we can steal, crack and hacked passwords. Fraudulent agencies can purchase user information and credentials. Several instances such as Yahoo security breach, LinkedIn data leaks, Drobox user account leaks, Facebook data leaks and many more are seen worldwide. Another reason could be to include applications and platforms that would force the user to collect increased passwords. As discussed in [25] a study was conducted which uses MAM Protocol for tool for encrypting authenticating sensor data. With the demand

branding, publicity and efficiency of the appliance, technology and its users are continuing to increase, secure channels are increasing to speak and store passwords [26-28]. While password-based registration has become more prevalent today, as internet-connected devices have increased dramatically and users have more Digital Accounts than it has ever been, password-less authentication [29] is a more applicable solution for a safe login to online accounts. Passwords can hardly be stored, and it would cause users to maintain a password for most applications that makes them hackers prone [30]. This is the reason for increasing security breaches and making it easier for hackers to capture data [30,31]. This also promoted applications that store all user accounts and passwords related to the user's respective local accounts [32].

1. Enhanced User Experience: New-age users need not remember puzzles or questions such as: "What's your first car?" "Who's your best friend?" etc. This reduces the registration time. They are more interactive than password-based authentication and have more services [33].

2. Improved Security: There is more stable improvised zero-password security to remember when we do not use passwords. The main dimension of any software development application is safety, which includes different authentication, verification, authorization, and integration processes. The user or the creator of the application should not ignore these factors when using or creating them. Over the past few years, a spike in security violations have led developers to develop more reliable techniques and authentication mechanisms. One such authentication method is the use of password less authentication. Users of this authentication service are no longer required to retrieve complicated passwords regularly for several applications. This form of authentication does not require a password to log into any program. Password-less authentication is all the rage, and it is making passwords obsolete by the day [33]

3. Authentication vs. Authorization: Authentication and authorization can sound similar, but in the world of identity and access, they are two different security mechanisms. Authentication verifies that the users are who they pretend to be. Authorization grants access to a resource to all users.

Parameters	Authentication	Authorization
What exactly does it does?	Checks credentials	Permissions are granted or denied
What is the mechanism behind it?	Passwords, biometrics, one-time pins, and smartphones are all options.	Security teams manage security settings.
Is the consumer able to see it?	Yes	No
Is the consumer willing to alter it?	No, but just partially	No
What is the process of data movement?	Using ID tokens	By means of control tokens

Table 1 Comparison of Authentication vs Authorization Methods

Table 1 shows the comparison of Authentication and Authorization methods. It also demonstrated the mechanism, consumer profile and the methods of data movement.

Authentication:
The act of validating the user is known as authentication. In every protection procedure, this is the first move. Authentication can be as simple as allowing anyone to download a specific file from a server or as complex as giving individual users administrative access to an application. Complete the following steps to complete the authentication process: Passwords include: - The most important authentication variables are usernames and passwords. The system assumes a user's identity is legitimate and grants access if they enter the correct data.

Authorization:
Authorization carried out with the purpose of authorizing a user to access a particular resource or feature during the security of a device. Access control and client privilege are two terms that are often used interchangeably.
Authorization must always come after authentication in a safe environment. Before an organization's administrators allow them access to the requested services, users must first prove their identities are authentic.

This review paper is divided into five sections. Section I. focuses on Traditional Authentication Methods, Section II covers Password-less Authentication, Section III describes Types of Password-less Authentication, Section IV briefs about the applications of Biometrics and Section V covers the Emerging Authentication Methods.

I. TRADITIONAL AUTHENTICATION METHODS

1. Universal Authentication

The process of checking who a user wants to be is known as authentication. You have also been asked to create a username and password every time you have signed up for a website. Since this is such a standard practice, it is almost second nature for some users to build accounts without giving much thought to the credentials they select [34].

Advantages
Simple to use and deploy, with almost no additional configuration needed since the OS provides user accounts and passwords. When using the SSH Tectia Connector, use a generic password.

Disadvantages
Security is fully supported, as is confidentiality and, as a result, password strength. Does not have a good identity check.

2. Two factor authentication (2FA)

Two Factor Authentication seems to be the technical term for a method of forcing a user to check their identity in two diverse ways before being given access to a device. Users have traditionally depended on and are familiar with authentication schemes that require them to provide a unique identifier, such as an email address, username, or phone number, as well as a valid password or lock, to gain access to the device [34]. 2FA builds on this paradigm by enabling the user to enter a one-time token that is dynamically generated and distributed via a process that only the user has access to. Another popular approach is to add a second factor based on the user's biometric data like fingerprints or retina. The most common method used by hackers is to learn a user's password or pin.

3. Multi-factor authentication (MFA)

(MFA) is a security function that allows a user to have two or more authentication elements to get access to a service, along with an app, an online account, or a proxy server [34]. A phone or other physical token owned by the user, intrinsic factors such as biometric traits, or something well-known, such as a passcode, are all examples. MFAs include ATMs, which include a card (physical token) and a PIN (something known) to complete a transaction. Multi-factor authentication can be part of a robust access control scheme. Rather than requiring login information, MFA needs use of one or more external authentication factors, which reduces the likelihood of a successful cyberattack [33].

Advantages

Users are first danger point for a network, so MFA alleviates user and IT admin anxiety by preventing sensitive data from falling into the hands of persistent hackers. If an intruder obtains a user's password to a device, they would be unable to gain entry because they lack the token. Computer-based 2FA guarantees that your data is not compromised if your device is lost.

Disadvantages

Unable to access a particular program or device if you do not have access to a TOTP generator and have not discovered backup tools for authenticating user access. When unable to access the computer, it will bring a one-time recovery MFA code with you. It is difficult to introduce MFA through an entire enterprise since it is typically left to the users to do so. IT administrators may not always be aware of an organization's MFA implementation.

4. Token Hardware Authentication

A protection token (also called an authorization token sometimes) may be a small hardware mechanism where the owner can access a network service. The gadget can also be in the sensitive type of card or may be included during a widely used item such as a key fob. Safety tokens provide an additional degree of assurance in a way called two authentications: the user features a personal number (PIN) to permit them, since the owner of that device; the device shows a variety of tokens to enable the individual to log on to the service [34]. The number is changed constantly for any person, normally about every five minutes. A protection token can be an entity, in contrast to a password.

Advantages

Standalone – does not require receipt, internet networking, or other tokens Stable – specially crafted hardware tokens to only create tokens. Secure – because these instruments execute only one mission, potential exploitation vectors are significantly reduced

Disadvantages

Costly for installation and maintenance Hardware – many computers are quickly misplaced, forgotten, or destroyed. So many devices - a multi-service hardware can render consumer unwilling to use 2FA

5. Software Authentication Tokens

Software tokens enable the user to download and update a program running on their machine or mobile device, which creates tokens for the user automatically. With the rise of smartphones, this approach is becoming increasingly popular. Software tokens function in the same way as hardware tokens, where they are created randomly and last quickly before you change but developers can select various applications to meet business needs [34,35].

Advantages

Applications normally have simple interfaces that only display the user token. Quick program updating and patches if necessary. Extensibility and improved feature capacity, such as the need for an app control pin or the use of a single application for several accounts.

Disadvantages

Costly to deploy and sustain. Additional software allows users to download additional software and to update it on their computers. Token-generating program can be exploited without user awareness.

6. Single Sign-On

Single sign-on is an authentication system which allows users to authenticate safely using only one set of passwords for various apps and websites. SSO is built on a trust arrangement between a service provider application and an identity provider. Typically, this confidence arrangement is founded on a certificate shared between the provider of identity and the service provider. This credential is also used to verify personal information sent from the ID provider to a service provider by that the service provider knows it comes from a reputable source [33-35]. SSO takes the form of tokens that define the user-specific details of the email address or username of a user.

Advantages

Streamlines user access to apps. Reduces the load to store several passwords. Easy to deploy and link to new data sources.

Disadvantages

Using a single password raises password insecurity probabilities. Access to all relevant systems is lost when SSO fails. Spoofing identity of remote account accesses.

7. OTP authentication

The method starts with the first user signing into a device with its username. This causes an on-demand OTP to be delivered to the telephone number or email address of the recipient, according to whatever distribution system the company has locally [34,35]. The user gets the OTP and enters it to check the identity of the user and get access. Unlike hard and soft OTPs, on-demand OTPs are mostly event based rather than time-based. However, like other OTP distribution systems, OTPs on demand are not reusable and expire after use.

Advantages

Low cost. Easy to use. No Crack Shared Secret. Ease of Administration

Disadvantages

Not NIST recommended. Enhanced Surface Attack. Might be spoofed. Can be hijacked by phone accounts. Can be intercepted codes. Codes send in plain text. Can be seen without permission. Shortcomings for mobile and messaging. Needs mobile or Internet access.

8. Push Notification Authentication

Push Notification Authentication allows authentication of the user by submitting a push message to a safe program on the user's computer to notify them of an authentication effort [33-35]. Users may display authentication information and allow or reject entry, normally by simply pressing a button. In-band or out-of-band notifications may be delivered through any range of channels of communication.

Push alerts authenticate the user by verifying that the authentication mechanism registered device normally a mobile device is currently owned by the user.

Advantages

Push alerts are much more comfortable than opening and copying the code for your authenticator software. They also have details on who is attempting to log in, including the type of device, IP address and general location. This warns you of any malicious login attempts if they occur.

Disadvantages

The authentication of push notification requires the Internet connection of your phone. Thus, you will not get a login prompt if you have no data link and are not wired to Wi-Fi. There is also a possibility that the facts in the drive will be ignored and automatically approved without thought. This could cause you to offer access to someone who should not have it if you are not careful.

9. Captcha Authentication

A traditional Captcha text has alphanumeric or twisted characters. To be checked, the user must type this in a text box. CAPTCHA stands for a fully automated public turning test to educate computers and people. To block spam, websites enforce Captcha. Spammers are attacking websites to sabotage spam data and expect to bring users back to their server [35]. Spam usually ends up with a denial-of-service DOS attack that can download the whole website or program. To prevent this, websites add Captcha that makes it difficult to run or log in to the website automatically. The twisted letters are readable by humans and can avoid spamming by programmed bots [35].

Advantages

Increases protection. Lower spam. Automatic blocks expanded use of utilities. Make online business safer. Differentiates between people and machines.

Disadvantages

Certain browsers fail. It is difficult to read at times. A challenge for disabled people. Time-consuming. Complete evidence not guaranteed.

10. Third Party Authenticator

A web-based authenticator that uses 2-phased authentication facilities to authenticate users of software using the TOTP AND HOTP. Authenticator creates a 6-to-8-digit unique password which must be entered in addition to their normal login information when signing into a website supporting Authenticator.

Advantages

The freedom to use different apps. Amazingly simple to use. Can be used on multiple computers. Ads an optional layer of password protection. The most widely acknowledged 2FA application on all websites.

Disadvantages

Functionality is different on multiple computer models. You cannot pass the codes to any other user. You will be locked from any accounts you set up to use for this app if you lose access to your device.

10. Enterprise Authentication Service

An Enterprise Authentication Service can be a single device authenticating users across a broad array of applications. The device asks the user to verify the user credentials when logged into a program that uses the Enterprise Authentication Service [35]. This centralizes the user identification and password storage by reducing password files spread across the company's application servers, which enhance the organizational security. It also decreases the total operating costs by centralizing user credentials administration.

Advantages

The global model of naming offers exclusive entries. Requires several separate folders to be used. Future/local standards can be expanded. Runs directly over TCP/IP and SSL. It has greater market sponsorship. The protocol is built on technology already applied. Most utilities such as TCP and DNS use LDAP. It is a protocol open source with a highly scalable architecture. LDAP is automated, so it is much simpler to upgrade than DNS.

Disadvantages

Directory servers must be LDAP compatible to deploy the service. LDAP is tough, but is seldom used, as opposed to simpler and commonly used DNS.

11. Session Based Authentication

When authenticating the session, the server can build a user session after the user logs in. The session id is then saved to the user's browser on a cookie. The cookie will be submitted with each subsequent request while the user logged in. The server then will match a session ID stored in the cookies with memory session information to check the user identity and transmit a response to the corresponding state [35].

12. Web Token Based Authentication

Often mobile apps use JWT instead of authentication sessions. The server generates a JWT key in the token-based program and transfers the JWT to the customer. The client stores the JWT (usually locally stored) and contains all requests with the JWT header. A server validates JWT for each client request and sends a response. The main change is that the user status is not stored on the server, as now the state is stored inside the token on the client end. For purposes such as mobile device authentication, most modern web apps use java web token for authentication [36].

13. Knowledge Base Authentication (Security Key)

Knowledge-based authentication can be a security action that detects end users by requiring them to answer safety issues to have accurate permission for web or digital activities. Knowledge-based authentication is common in many distinct kinds of network environments and around the internet, where businesses often insist that users answer these questions to have access to confidential, password-protected parts of a site [35,36].

Static and Dynamic KBA

If you ever had to restore a password, you had a static KBA. You select security issues with this approach and have responses that are saved and referenced later. In this kind of KBA, the consumer monitors questions and responses. Dynamic KBA can be a high degree of authentication using information requests to check each user identity, but it does not enable an individual to provide questions and answers in advance. Questions such as marketing statistics, credit reports or transaction records are compiled from public and personal data.

Advantages

Well known by consumers., Questions collected over 30 years, Questions need to be answered within a fixed time.

Disadvantages
Quick to find answers through social networking and social engineering platforms. Fraudsters can buy illegal market responses from KBA. Questions often generated based on credit office information. Recent PII exposure infringements. Specific countries exclusive. Also, the customer interface is bad. Do not depend on government IDs, there is a shortage of jurisdiction. Some consumers find it interfering.

II. PASSWORD LESS AUTHENTICATION

Password less Authentication is a way to authenticate a user in a computer system without inserting a password or other knowledge-based secret. Password less authentication depends on a key pair – a personal and a public key. The public key issued by the authenticating service during the registration (remote server, program, or website) is stored in private keys and is only available if a biometric signature, hardware token or other element without password is added. Users are invited to enter their public identification (Username, telephone number, E-mail address or other registered ID) in the most popular implementations, and then complete the authentication process by proving their identity in the type of authentication element that is accepted. These considerations usually fall into two categories: Auth0 (2021) Some designs can also accept a combination of other variables including geo-location, addresses of the network, behavioral behaviors, and movements. Password less authentication is usually mistaken for Multi-Factor Authentication (MFA), and both use good kinds of authentication factors, but although MFA is used as another safety layer above and above password-based authentication, password less authentication has no secret and uses only a secure factor to make the identity authenticated faster and faster. Auth0 (2021) "Password less MFA," where all methods are used, is used and then the authentication flow is password less and uses several variables, offering the maximum degree of protection when fully applied. Auth0 (2021)

Working:
Analogous of digital certificates is the technology behind password less login. Cryptographic key pairs include a personal and public key. Consider the public key because of the padlock to see how this works. In the other side, the private key unlocks the clock. In short, there is only one key to the slot and, reciprocally, a slot for the key. This ensures that a public-private key pair must be created if a user wants to make a protected account. This is mostly achieved by platforms like a smartphone application or a plugin extension. Here are the following steps: Private keys stored on a local user's computer and attached to a PIN, fingerprint, or facial recognition authentication factor. On the other side, the public key passes to the website or service where the user wants to login.

Advantages
Greater protection, password, due to reuse, sharing, hacking, etc. is a vulnerable point in computer networks and is used as a top attacking vector responsible for an incredibly high percentage of security breaches. Better service for users, in addition to remembering complex passwords and complying with various safety protocols, users are not expected to renew passwords regularly. Reduced IT costs, since IT teams no longer need to store and maintain their IT keys, track the leaks, reset the missing passwords, and comply with the password storage rules.

Disadvantages
Costs of implementation, while password less authentication is agreed to lead to savings overall, implementation costs remain a hindrance to many potential users. The cost of deploying an authentication method in an existing directory is correlated with the need to often install additional hardware (e.g., OTPs or security keys). Trainings and skills necessary as most password protection schemes are similarly designed and used for several years, password less authentication allows both IT teams and end-users to adapt. An error, specifically applications using OTP or mobile device alerts may create a problem for end users when a device is disabled, lost, stolen, or simply upgraded.

Password less authentication improves security, increases brand effectiveness, and saves valuable IT resources by eliminating the use of passwords. Single sign-on (SSO), traditional multi-factor authentication (MFA), and similar methodologies have their own legacy benefits, but they can all be circumvented through methods such as phishing, keylogging, password spray, or brute force attacks.

III. TYPES OF PASSWORDLESS AUTHENTICATION

1. Social login Authentication

Social login may be a single sign-on using existing information from a social networking service like Facebook, Twitter, or Google, to sign into a third-party website instead of creating a new login account specifically for that website. It is designed to simplify logins for end users also to provide increasingly reliable demographic information to web developers.

Advantages
Pre-validated, Account linking, Faster registration Goal-targeted content, Multiple identities, huge amount of visitor data, Personalized experiences, Possible less failed logins

Disadvantages
Social logins can contain false information (data accuracy) Social networks/logins are sometimes blocked Loss of control to a third-party Lack of email addresses for the client service Visitors forget which social login they have used

2. MAGIC LINK AUTHENTICATION VIA EMAIL

The user must enter an email address in this type of authentication. If the user submits their e-mail address, an identification key is given and kept in the framework for potential reference. The e-mail with the assigned URL will be sent to the recipient, and a URL that can be used as a token will be sent to it. If the user clicks the key, your server verifies that the token and creates a new long-term token, which is saved in your database. As a precaution, it is recommended that the connection be enabled for the user for no more than 3 minutes.
Figure 2 describes the application requests the user to enter the email address. In the second step, the user enters the email address. The third step is to call the API of password less server and share unique user identification number with Auth0 which verifies the user details in the database and sends the user unique one-time password accessible link on

the users registered email address via Mail Server in the 4th registered email address in the 4th step. A unique one-time link is received by the user to authenticate himself as the authorized user once it's done user can access the application without using any kind of password.

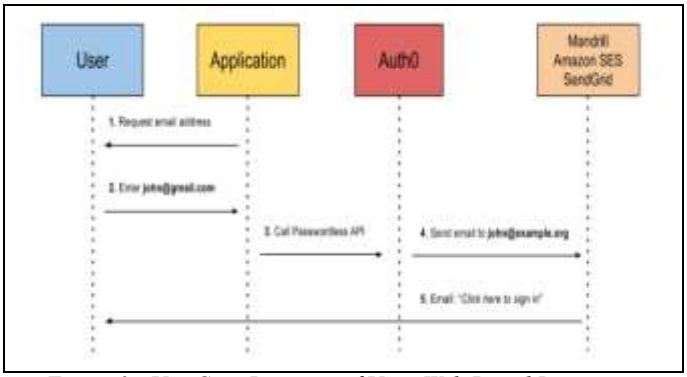

Figure 2 : Use Case Diagram of User-Web Portal Interaction

3. One-Time code Authentication via Email

The user must enter an email address in this type of authentication. The customer receives an email containing a single, one-time code. When a user enters this code into the application, it is checked, a session is launched, and the user is signed in [37].

Advantages

Users can accept emails from both computers and mobile devices, making it very user-friendly. Setup and maintenance costs are low. Options, for example, will provide the user with additional options for verifying the token, such as clicking a connection.

Disadvantages

Email delivery will fail for a number of reasons, including being labelled as spam, being bounced by the server, getting the delivery queue backed up, and so on. Emails can be intercepted by third parties, and tokens can be hacked. Redundancy: Once a third party has access to a user's passwords, they could be able to access their email as well, enabling them to quickly acquire the token [38,39].

Figure 3 describes Use Case Diagram of User- Auth0 process. It describes in step one user enters code in applications to access the account but as applications is using third party authenticator it will call API of Auth0 in step 2, then in step 3 Auth0 verify the user and creates an user connection. In step 4 user got authenticated, now he can access the application

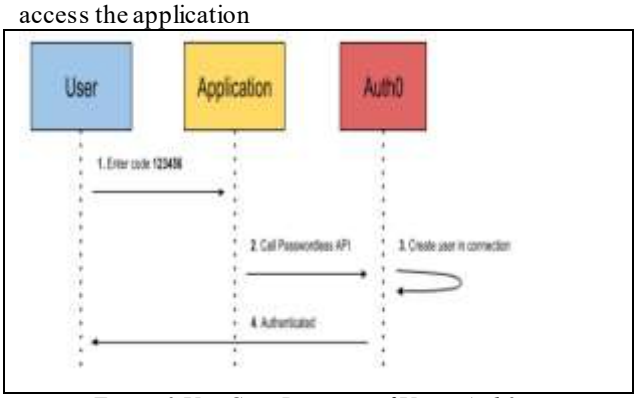

Figure 3 Use Case Diagram of User- Auth0 process

4. One-Time Code Authentication via SMS

The user must enter a valid mobile number in this type of authentication. The phone number is then given a one-time code that is exclusive. When a user enters this code into the app, it confirms that the code is right and that the mobile number is legitimate and belongs to a user. A session is then started, and the user is logging in.

Advantages

Most phones have SMS features most people are happy accepting text messages. It is also inexpensive to set up and manage.

Disadvantages

To collect the token, you will need a mobile signal and reception. Third parties could be able to intercept SMS communications. Since a physical device is needed, the user unable authenticate if their phone is lost or stolen.

5. Biometric Authentication

Biometric authentication is a method of protection that compares and tests a user's biometric features to ensure that the person attempting to enter a computer is allowed to do so. Biometric features are physical and biological traits that are unique to a particular person that can be instantly compared to approved features contained in a database. Access to a tool is given if the biometric characteristics of a person attempting to access it match those of an authorized user. Biometric authentication can also be used to monitor entry points such as doors and gates in physical environments. Market electronics, especially computers and smartphones, are increasingly incorporating biometric authentication. Biometric identification systems are also being used in protected environments by governments and private companies, such as military bases, airports, and ports of entry while approaching national boundaries. Fingerprint scanners, the digital equivalent of traditional ink and paper fingerprinting, work by capturing the distinctive swirls and ridges that make up each person's fingerprints.

Advantages

Used in a variety of industries. Among the most often used modalities.

Disadvantages

Performance may be hampered by the fingerprint's consistency or current circumstances, such as damp or dusty fingertips [39]

6. Facial Recognition

Facial recognition technology produces faceprints by comparing hundreds of distinct measurements from an authorized mask to the face of a person attempting to obtain entry. Access is allowed if enough dimensions from a patient fit the authorized face, like fingerprint recognition. Facial recognition has been applied to a variety of smartphones and other common products, but it can be inaccurate when matching faces when seen from different angles or when attempting to discriminate between individuals that look alike, such as close relatives.

Advantages

Mobile devices are commonly used, and the majority, if not all, of them have cameras. They need extraordinarily little configuration. These capabilities are included as basic features on most modern mobile devices. One of the most convenient biometric identification methods is facial recognition.

Disadvantages

Face detection devices are not always made equal. Others are more easily spoof able than others. Third-party or proprietary implementations are more successful than device-native solutions. Active liveness identification in facial recognition systems allows the user to turn their head, blink, or execute other acts in the moment to validate the order. This method is easier for an attacker to analyze and bypass, and it can result in a frustrating user interface, while "passive liveness identification" happens behind the scenes and is more difficult for an attacker to recognize and understand.

7. Voice Identification

Individuals can be distinguished using voice recognition technology, which tests vocal characteristics. They merge several information points to create a voiceprint profile to fit to a database, like facial scanners. Voice recognition systems excel in assessing and analyzing a speaker's mouth and throat for the creation of unique shapes and sound characteristics, rather than "listening" to a voice. This method removes the dangers involved with trying to disguise or imitate a sound, as well as general factors such as illness or time of day, which can modify the audial qualities of a voice to a person's ear. The terms a user speaks to gain access to a voice-protected computer may be generic, acting like a sort of password and making it simpler to compare accepted voiceprints to a user's unique voiceprint, as well as foiling specific methods to circumvent voiceprint comparison, such as capturing a registered user saying anything irrelevant.

Advantages

Provides a simple authentication process. Some applications also provide an expression for the recipient.

Disadvantages

Background noise can cause records to be distorted. Speech distortion and authentication may be caused by the common cold, bronchitis, or other common illnesses. In public settings, a person can be reluctant to talk aloud (such as on a train or bus).

8. Eye Scanners

Eye scanners of several types, such as iris scanner and retina scanners are commercially available. Retina scanners operate by reflecting a blinding light through the eyes, creating noticeable vessel shapes that can be read by the scanner and matched to accepted data stored in a database. Iris scanners work in a same way, looking for different patterns in the color ring around lens of the eyes. Both types of eye scanners are good for hands-free verification, but they can be inaccurate if the subjects are wearing contact lenses or glasses. Photographs have also been known to deceive eye scanners, but as scanners grow more advanced and integrate variables like eye activity into their authentication systems, this approach is likely to become less feasible.

Advantages

Eye recognition can be as swift and precise as facial recognition in some cases (though less user-friendly).

Disadvantages: When in direct sunshine, getting a sample for comparison can be difficult (pupils' contract). It can necessitate specialized hardware depending on the implementation.

IV. APPLICATIONS OF BIOMETRICS

Authorities have traditionally used biometrics for military access management, criminal or civil authentication, both under a highly supervised legal and technological context. Today, businesses such as banking, online shopping and retail display a strong demand for biometrics' benefits. Most notably, more mobile users are opening their phones with a fingerprint or a face, which has increased recognition and adoption in the last seven years.

Use cases of biometric authentication

Law enforcement and public security, Civil identification, Border, migration control and travel Military, Healthcare and subsidies, Banking financials services, Commercial applications, Physical and logical access

Advantages of biometrics

Whatever approach is used; both biometric methods have one thing in common: they all capture universal human traits that can be seen in all people. They are one-of-a-kind, and they encourage one person to be differentiated from another. They are permanent, and they do not adjust over time. Ready to be recorded (with or without consent). Measurable, allowing for contrast in the future. Forgery-resistant (a face, a fingerprint).

Disadvantages

Security, fingerprints, and other biometric information may be compromised and cannot be altered.

Privacy, the preservation of biometric data poses privacy issues. Additional hardware is used to validate biometric information such as cameras, scanners, and other equipment.

Biometric future

New biometric protection technologies are being implemented in response to data theft and document misuse, extremism and cybercrime, and international regulatory reforms. Increased consumer awareness, huge performance improvements, an upscale bid, and declining costs of scanners, IP cameras, and applications all help to make biometric systems more appealing. Biometrics are often identified as the most practicable means of reliably and quickly identifying and authenticating individuals based on specific biological characteristics. [39]

As mentioned in the article [40], the Global Password Less Authentication market size is estimated to be USD 35.48 billion in 2019 and is predicted to succeed in USD 456.79 billion by 2030 with a CAGR of 29.1% from 2020-2030 Password less authentication is a security method that verifies an individual's authenticity by using a few special biological characteristics [41]. It is a way of verifying a user's identity that does not require the use of passwords. Password less authentication has a range of advantages, including better user interface, enhanced reliability, and lower overall cost of ownership. Both human and computer samples of biometric data can align to ensure confirmation [42,43].

Market Analysis

- The EMA (Enterprise Management Association) performed key, survey-based research with IT experts who are familiar with the administration and usage of identity and access management services in their organizations. To maintain

credibility, all respondents were vetted, and statistical findings were determined to be within a 5% margin of error. They discovered the following information from the survey.

- The overall number of respondents was about two hundred.
- Inside their companies, 56% percent of respondents held executive-level posts.
- Respondents came from a wide variety of sectors, with high technology, engineering, financial services, healthcare, banking, retail, and education accounting for 81 percent of the total.
- Respondents came from a variety of businesses of varied sizes.
- Small companies with more less than 1,000 employees account for 37.5 percent
- Medium businesses with 1,000 to 7,500 employees account for 39.5 percent
- Big businesses with more than 7,500 employees account for 23 percent.
- 96.5 percent of those who responded said they were geographically in North America.

Key findings

- Low-friction authentication systems improve security efficiency while also reducing administration activities and costs.
- Password less security systems are commonly accepted as delivering the most frictionless user interfaces.
- The use of identification protocols (such as FIDO and SAML) and alignment of advanced identity management systems has been identified as the most significant obstacle to password less authentication technology adoption.
- The new buzzword in secure authentication for IAM solutions is password less authentication. It is a worthy cause. Consumers and others attempting to protect client and business data continue to be vulnerable to passwords. Faulty or compromised passwords are used in 81 percent of data breaches. And cyber criminals' number one priority is passwords.
- Passwords are a headache for IT agencies in a variety of areas. They must first store the passwords in a safe manner. Failure to do so threatens a breach, which will have a significant effect on the company's bottom line, share prices, and, as a result, its integrity for years to come. Second, as the keeper of passwords, you are just responsible for their support. This also entails dealing with a deluge of password reset requests.
- But there is a legitimate justification for companies to allow users dump their passwords and turn to password less authentication.

V. EMERGING AUTHENTICATION METHODS

1. ADAPTIVE AUTHENTICATION

Risk-based authentication is another name for adaptive authentication. When authenticating, adaptive authentication considers external variables such as context and behavior, and these values are often used to attach a risk tier to the login attempt. The risk level is measured depending on how certain questions are answered, and it is used to decide if a user will be asked for a second authentication factor or if they will be able to log in at all. As a result, risk-based authentication has become a popular concept to characterize this form of authentication. With Adaptive Security in effect, a user signing in late at night from a restaurant, which is not something they usually do, could be needed to enter a code texted to their phone in addition to their username and password. When they log in from the office at 9 a.m. on a weekday, they are merely asked for their username and password.

2. Transaction authentication (location based)

Unlike other web authentication approaches, transaction authentication takes a different approach. Rather than relying on details provided by the customer, it applies the user's features to what it already knows about the user, looking for differences. Consider the case of a buyer with a Canadian address on an online sales website. A transaction authentication system can search the user's IP address as they log in to see if it suits their known location. All is fine if the consumer is using a Canadian IP address. However, if they are using a Chinese IP address, anyone might be attempting to impersonate them. In the latter scenario, a red flag is raised, prompting further verification action. Of course, the customer could be visiting China, but a transaction security scheme can protect them from being fully shut out. Instead of replacing password-based schemes, transaction authentication adds another layer of protection.

3. Computer recognition authentication

Transaction authentication is close to machine recognition authentication. By verifying if a person is on a particular device, computer recognition verifies that user. The first time a consumer logs in, these systems mount a small device plug-in on their machine. A cryptographic interface marker is used in the plugin. The marker is tested the next time the user checks in to make sure they're on the same computer. The beauty of this method is that it is completely invisible to the user, who merely inserts their username and password, with authentication taking place automatically. Users can switch devices, which is a drawback of machine recognition authentication. Other types of authentications must be supported by such a framework to allow logins from new devices (e.g., texted codes).

4. Certificate-based authentication

Digital certificates are used in certificate-based authentication technologies to verify users, computers, and devices. An electronic certificate is a digital document that resembles a driver's license or a passport in appearance. The credential includes a user's digital identity, like a public key, as well as a certification authority's digital signature. Only a credential authority may grant digital certificates to show possession of a public key. When users sign into a server, they must have their digital certificates. The server

verifies the digital signature's and, as a result, the certificate authority's integrity. The server then hires encryption to ensure that the user has a legitimate private key for the certificate.

VI. CONCLUSION AND FUTURE WORK

There is really no denying that passwords in recent years have been even more vulnerable to compromise. Password less authentication helps to remove vulnerabilities to authentication. This new study of password less links demonstrates an increase in password less adoption. In comparison, password less authentication is extremely helpful and gains ground in the IoT environment. The authentication of an IoT system with a touch ID, a push notification, or even one-time passcode is faster, safer, and quicker than conventional means. Adapt offenders and compliance checks are typically short-lived. This also leads to a long-term view that promotes stability, anonymity, sustainability, user interface, scalability, and inclusiveness of the sound-authentication scheme. The future of authentication will follow several paths that we are just starting to pursue including self-sovereign identities in Blockchain and zero faith networks. However, the imminent journey to launch platform companies leaves passwords behind.

REFERENCES

[1] Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020, May). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy* (pp. 268-285).

[2] C. Herley, P. C. van Oorschot, and A. S. Patrick, "Passwords: If we're so smart, why are we still using them?" in FC, 2009.

[3] Zwane, Z. P., Mathonsi, T. E., & Maswikaneng, S. P. (2021, May). An Intelligent Security Model for Online Banking Authentication. In *2021 IST-Africa Conference (IST-Africa)* (pp. 1-6). IEEE.

[4] Matiushin, I., & Korkhov, V. (2021, December). PASSWORDLESS AUTHENTICATION USING MAGIC LINK TECHNOLOGY. In *CEUR Workshop Proceedings* (Vol. 3041, pp. 434-438). RWTH Aahen University.

[5] Firdous, A., Rehman, A. U., & Missen, M. M. S. (2021). A gray image encryption technique using the concept of water waves, chaos and hash function. *IEEE Access*, *9*, 11675-11693.

[6] Verizon Data Breach Investigations Report. Available at: https://www.verizon.com/business/resources/reports/dbir/ (accessed 05.09.2021)

[7] 2017 Consumer Mobile Security App Use. Available at: https://www.keepersecurity.com/ (accessed 05.09.2021)

[8] J. Bonneau, C. Herley, P. van Oorschot, and F. Stajano. Passwords and the evolution of imperfect authentication. Commun. ACM, 58(7):78--87, 2015

[9] J. Bonneau, "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, 2012, pp. 538-552.

[10] J. Bonneau and S. Preibusch, "The password thicket: technical and market failures in human authentication on the web," WEIS '10: Proceedings of the 9 Workshop on the Economics of Information Security, 2010.

[11] F. Stajano, "Pico: No more passwords!" in Security Protocols Workshop. Springer, 2011.

[12] S. Aebischera, C. Dettoni, G. Jenkinson, K. Krol, D. Llewellyn-Jones, T. Masui, and F. Stajano, "Pico in the wild: Replacing passwords, one site at a time," in 2nd European Workshop on Usable Security (EuroUSEC '17), 2017.

[13] A. Deveria. (2019, May) Can i use webauthn? [Online].

[14] B. Girardeau. (2018, May) Introducing webauthn support for secure dropbox sign in. [Online]. Available: https://blogs.dropbox.com/tech/2018/05/introducing-webauthn-support-for-secure-dropbox-sign-in/

[15] A. Simons. (2018, Nov.) Secure password-less sign-in for your microsoft account using a security key or windows hello. [Online].

[16] B. Wong. (2019, May) WebAuthn: The future of device based 2FA at Twitter. [Online].

[17] Microsoft. (2018, Jul.) Web authentication and windows hello. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-edge/dev-guide/windows-integration/web-authentication

[18] M. Wielgoszewski. (2019, May) Securing your gemini account with webauthn. [Online]. Available:

[19] A. Powers. A node.js library for performing fido 2.0 / webauthn server functionality. [Online]. Available: https://github.com/apowers313/fido2- lib

[20] Y. Ackermann. (2019) Webauthn awesome: A curated list of awesome webauthn/fido2 resources. [Online]. Available: https://github. com/herrjemand/awesome-webauthn

[21] Yubico. (2019) Developer program. [Online]. Available: https://developers.yubico.com

[22] C. Brand and E. Kitamura. (2019) Enabling strong authentication with webauthn. [Online]. Available: https://developers.google.com/web/updates/2018/05/webauthn

[23] Y. Mehta. (2019, May) Windows hello fido2 certification gets you closer to passwordless. [Online].

[24] A simple webauthn / fido2 javascript application. [Online].

[25] Gangwani, P., Perez-Pons, A., Bhardwaj, T., Upadhyay, H., Joshi, S., & Lagos, L. (2021). Securing Environmental IoT Data Using Masked Authentication Messaging Protocol in a DAG-Based Blockchain: IOTA Tangle. *Future Internet*, *13*(12), 312.

[26] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[27] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[28] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[29] K. Elissa, "Title of paper if known," unpublished.

[30] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[31] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[32] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[33] Chowhan, R. S., & Tanwar, R. (2019). Password-Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites. In *Machine Learning and Cognitive Science Applications in Cyber Security* (pp. 190-212). IGI Global.

[34] Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems*, *106*, 1-14.

[35] Matyáš, V., & Říha, Z. (2002). Biometric authentication—security and usability. In *Advanced communications and multimedia security* (pp. 227-239). Springer, Boston, MA.

[36] Vallabhu, H., & Satyanarayana, R. V. (2012). Biometric authentication as a service on cloud: novel solution. *International Journal of Soft Computing and Engineering*, *2*(4), 163.

[37] Rassan, I. A., & Al Shaher, H. (2013). Securing mobile cloud using finger print authentication. *International Journal of Network Security & Its Applications*, *5*(6), 41.

[38] Nojima, S., Susaki, E. A., Yoshida, K., Takemoto, H., Tsujimura, N., Iijima, S., ... & Ueda, H. R. (2017). CUBIC pathology: three-dimensional imaging for pathological diagnosis. *Scientific reports*, *7*(1), 1-14.

[39] M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). Totp: Time-based one-time password algorithm. *Internet Request for Comments*, 685E.

[40] Satheesh, M., and M. Deepika. "Implementation of Multifactor Authentication Using Optimistic Fair Exchange." Journal of

Ubiquitous Computing and Communication Technologies (UCCT) 2, no. 02 (2020): 70-78.

[41] Kumar, Dinesh, and Dr S. Smys. "Enhancing Security Mechanisms for Healthcare Informatics Using Ubiquitous Cloud." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 2, no. 01 (2020): 19-28.

[42] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[43] Vivekanandam, B. "Design an Adaptive Hybrid Approach for Genetic Algorithm to Detect Effective Malware Detection in Android Division." Journal of Ubiquitous Computing and Communication Technologies 3, no. 2 (2021): 135-149.