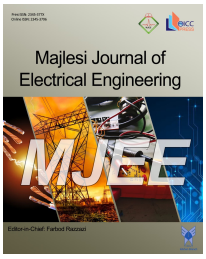

Volume 19, Issue 2, 192544 (1-13)

Majlesi Journal of Electrical Engineering (MJEE)

https://doi.org/10.57647/j.mjee.2025.1902.44

Innovative passwordless authentication approaches in IoT identity management

Venkatrao A. Kommuri[1], Kareemulla B. Shaik[2,*]

[1]*Department of CSE, LakiReddy Bali Reddy College of Engineering, Mylavaram, NTR DT, 521230.*
[2]*School of Computer Science and Engineering VIT-AP University, Amaravati, Andhra Pradesh-522237.*

[*]**Corresponding author:** kareemulla.shaik@vitap.ac.in

Review Paper

Received:
11 December 2024
Revised:
12 January 2025
Accepted:
28 February 2025
Published online:
1 June 2025

Abstract:

A global ecosystem of networked sensors, actuators, and other devices intended for data exchange and interaction is known as the Internet of Things (IoT). Password-based authentication has been a major component of IoT solutions historically, despite its numerous flaws. This survey article provides a thorough analysis of the literature with an emphasis on the implementation of authentication without the use of passwords on the Internet of Things. Ensuring that authorized persons have the correct access to related IT incomes under the correct situations is the core necessity behind enterprise IoT security. Identity managing, the first line of protection in initiative security, is a key component of this project. Traditional password-based authentication systems are frequently regarded as "high friction," causing users' problems and lengthy procedures in addition to being vulnerable to different security threats. IoT businesses are investigating password less authentication techniques more frequently in an effort to improve user productivity while preserving strong security assurance in response to these difficulties. A comprehensive analysis of password less authentication mechanisms designed for the Internet of Things is presented in this article.

Keywords: Traditional authentication; Password less authentication; Emerging authentication; Biometrics; Web security

1. Introduction

The use of usernames and passwords has been the standard technique of internet authentication for decades globally [1, 2]. Unfortunately, there are a lot of security flaws in password-based online authentication. Remarkably, weak or repeated passwords are responsible for a significant percentage of online data breaches [3]. As a result, scholars and professionals have been working for a while to develop substitute authentication methods that provide increased security without becoming more difficult to use or install [4]. Federated identity systems(FID), such as single sign-on (SSO), are an example of such alternatives. SSO, in theory, improves security by decreasing password reuse and relieving the strain of remembering numerous passwords. However, consumers' privacy concerns have hindered its uptake outside of organizational contexts [5–7]. In a similar vein, the use of password managers has grown in status due to recommendations from security experts [8]. By helping customers generate, remember, and enter distinct passwords for every online account, these tools help users cut down on the number of weak and reused passwords [9]. Password manager adoption rates, however, have stayed comparatively modest [10].

A particularly interesting solution in the ongoing effort to replace traditional passwords for web authentication is the recently developed FIDO2 standard [4, 5, 9]. Public-key cryptography is used by FIDO2 in place of passwords. Instead of inputting their username and password when registering on a website, users use an authenticator—a piece of dedicated hardware or software that complies with the FIDO2 specification—to create a pair of public and private keys. The web application then receives the public key from the client. FIDO2 has a number of significant benefits. Users are freed from the hassle of remembering passwords, which improves usability. FIDO2 provides security by protecting users against remote assaults such as phishing and credential stuffing. Moreover, FIDO2 improves user privacy protection overall by reducing the centralized privacy issues connected to federated identification systems [11].

FIDO2 is supported by Chrome, Firefox, Edge, and Safari [12–14], and more websites are following [8, 15]. Two types of authenticators are needed for FIDO2. Platform authenticators connect to flexible client devices and authenticate just those devices. For iPhone and Mac laptop

online logins, Touch ID and Windows Hello can be used as FIDO2 platform authenticators. Customers have the unenviable task of signing up for a website multiple times, once on each of their devices. A USB security key is an example of a roaming authenticator that can be used on any device [16]. Roaming authenticators permit authentication on many devices, although users are typically apprehensive about bringing physical security keys such as USB sticks. [17–19].

Secure password management channels are emerging due to rising technology demand and user security concerns [20–22]. Password-based registration is still prevalent due to the development of internet-connected devices and digital accounts; however, passwordless authentication is safer and more practical for online account logins.

Chakraborty et al. [23] developed Sim FIDO, which employs simTPM, a SIM-card-based Trusted Platform Module (TPM), to construct hardware authenticators for Android devices. A new Android system service called External FIDO Request Receiver Service (XFRR) was developed by the authors to relay CTAP commands to the SIMTPM. A SIM card (authenticator) can be used in place of a standard credential on many devices. Passwordless authentication verifies a user's identification without a password. It uses safer methods like one-time passwords (OTP) and registered devices, or biometrics like fingerprints and retina scans. Traditional passwords are insecure, hard to remember, and easily lost. 90% of breaches involve weak or stolen passwords, making them a tempting target for cybercriminals. Password less authentication lets people log into a smart device without a password or other secret. Users often provide their public identifiers (e.g., usernames, phone numbers, email addresses) and then provide a secure confirmation of identity via a registered device or token.

Password-less authentication relies on a public-key cryptography infrastructure, in which a user's device (a computer, smartphone, or external security token) stores a private key that can only be accessed with a biometric signature and a public key is shared during registration with the authenticating service (a remote server, application, or website). This literature review articles are collected from google scholar from the year 2012 to 2023 May, all conference papers are eliminated only considered most relevant journal papers with good impact score. This literature review is broken up into four parts.

Section 2 is all about traditional authentication in Internet of Things settings.

Section 3 talks about authentication without a password.

Section 4 gives a full picture of password-based and password-less authentication methods.

Section 5 discusses New Authentication Methods.

2. Focuses on traditional authentication in internet of things environments

User and sensor nodes in the IoT network face many dangers. User authentication techniques must meet security and functional requirements to secure the IoT network [24, 25].

- Anonymous Users: The authentication mechanism should protect user privacy by preventing attackers from discovering their genuine identities.
- Unlikability: The approach must stop attackers from following what users do, protecting their privacy.
- Mutual Verification: Scheme participants must perform mutual authentication to verify each other's legitimacy.
- Session Key Agreement: The authentication scheme shall generate a new session key for message encryption and decryption with forward secrecy.
- Attack Resistance: The authentication technique must meet important security goals and withstand a variety of known assaults.

The recent rapid growth of the IoT has exacerbated security concerns. IoT uses identity identification to protect data and device availability. Scholars have developed IoT authentication algorithms, but resource-constrained devices cannot afford them. Notably, the constant upgrading of computer hardware has increased the key length of cryptographic systems, making it difficult for IoT devices to stay up due to the requirement to balance cost and usefulness. Physical limits, including energy, electricity, and communication link bandwidth, limit compute and communication capabilities despite recent storage capacity advances. Many scientists have studied IoT authentication techniques, typically neglecting anonymity [26–28]. Aman et al. [29] developed a certification approach that uses dynamic energy-quality trade-offs to implement different security levels based on security needs, lowering resource consumption. However, this method lacks anonymity and requires two data transfer rounds for authentication.

Wazid et al. [30] created a safe way for remote users to log in and set up keys in smart houses for devices that don't have a lot of resources. It protects anonymity against attackers eavesdropping on authentication messages, but not disguised attackers. He et al. [31] came up with a way to authenticate users anonymously over wireless body-area networks. This method stopped identity attacks in single-server designs but not in multi-server designs because key pairs had to be stored for each server. A cloud-aided, lightweight, anonymous certificateless authentication system for wireless body-area networks was developed by Shen et al. [32]. Conventional cloud deployments are remote from devices, delaying offload, especially for computationally expensive workloads. Edge computing research has grown because splitting and delegating difficult activities to other devices reduces computational overhead [33–35]. Yao et al. [36] developed a blockchain-supported, lightweight anonymous authentication mechanism for distributed virtual file systems. However, Xu et al. [37] stated that edge computing terminals may need to modify sensitive data, which could leak data during service offloading. Adding personal biological data and smart cards to authentication processes is another option [38, 39]. This method works better for

human-centric systems than device-centric ones.

Bilinear pairing's unique features make it promising for anonymous authentication [40, 41]. Constrained devices still find bilinear pairing procedures resource-intensive. Zhong et al. [42] devised a privacy-protecting authentication technique that precomputes and caches crucial data on resource-constrained devices before authentication to reduce process time. All intermediate results must be changed for each anonymous authentication; hence, the technique does not considerably reduce the computing workload. Since Chaum and Heyst proposed group signatures for anonymous authentication in 1991, they have been used in many scenarios [43–46]. Smart grids now have incentive-based demand response privacy protection from Gong et al. this approach uses discrete logarithms to construct pseudonyms and ring signatures to hide user identities during registration. The preset ring limits flexibility. Blind signature techniques have similar disadvantages [47]. Recent emphasis has focused on lattice-based signature methods in anticipation of quantum computing [48–50]. Despite having reduced signature size and improved security, they lack lightweight optimization for most IoT devices.

Military applications require secure sensor nodes to monitor deployments and enemy infiltration. WSNs are crucial in these settings, and their security is crucial because of their vulnerability to malicious assaults. Compromised sensors fail to monitor enemies and reveal confidential information. WSNs now gather and transmit sensitive data about household routines like power and water usage, patient monitoring, and elderly and child supervision. WSN applications in homes must contain strong privacy protections because most families are reluctant to share personal information. Wireless sensors in residences can track water and electricity use and household activities. However, these sensors can accidentally divulge family data, like when every person is away or when somebody takes a bath. Thus, data privacy must be protected [51–55].

Das [56] proposed the first smart card-based mutual authentication protocol for Wireless Sensor Networks (WSNs) in 2009, paving the way for authentication protocols in this sector. The protocol's inability to provide reciprocal authentication and user anonymity was eventually discovered as a security vulnerability. O-Sharif et al. [24] and Mishra et al. [25] independently introduced hash function-based WSN identity authentication techniques with better performance. In addition, Li and Hwang [57] presented a remote user authentication system based on biometrics that uses random numbers instead of timestamps to avoid clock synchronization. This protocol improved the user experience by allowing password changes. However, Das [58] found design faults in their approach, such as failing to validate the user's password at the start, which added communication and processing overhead. Direct biometric hashing increased the risk of biometric authentication failure during login and password changes which is shown in figure 1. Das developed a three-factor authentication system to address these difficulties. An [59] examined Das's protocol [58] and found it vulnerable to attacks, particularly in failing to offer mutual authentication. An improved mutual authentication scheme reduced attempts to impersonate users or guess passwords which is shown in below Table 1.

Li et al. [60] found that the system [58] was vulnerable to counterfeiting and lacked session key agreement. They then created a biometric mutual authentication and key agreement methodology. Khan et al. [61] investigated An's method [59], finding weaknesses and designing a more secure variant. Adding a protocol, Ibjaoun et al. [62] enhanced An's scheme [59]. Using XOR and hash algorithms, Turkanovic et al. [63] developed a password-based wireless sensor network mutual authentication system. Unfortunately, backward secrecy, impersonation attacks, and spoofing of sensor nodes were discovered by Chang and Le [64]. After identifying these flaws, they devised a plan to address them while simultaneously reducing storage costs and enhancing the effectiveness of the protocol.

Amin and Biswas [65] highlighted Turkanovic et al.'s

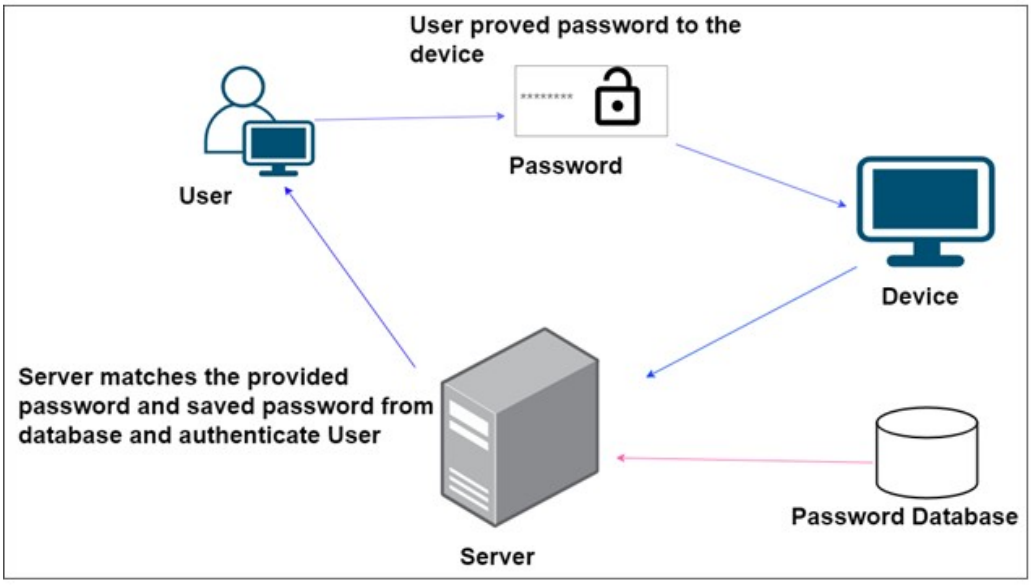

Figure 1. Traditional authentication.

Table 1. The following table comparison of Traditional Authentication.

S.NO	Scheme	Three-factor biometric key agreement for distant user authentication.	An anonymous mutual authentication technique that is both lightweight and physically secure.	A biometric server-to-server protocol for exchanging authentication keys.	Fingerprint biometrics are used in a two-factor authentication and key agreement technique.	A mutual authentication and key agreement system that doesn't require the use of shared passwords.
1	Key agreement and authentication that works both ways.	√	√	√	√	√
2	Assaults using commonly known session keys continue unabated.	√	√	√	X	√
3	Man-in-the-middle attacks occurring constantly.	√	√	√	√	√
4	Safeguarding against actual assaults.	X	√	√	X	√
5	Long-term safety with no gaps.	√		√	√	√
6	Attacks aimed at stealing mobile devices continue.	X	√	√	X	√
7	Passwords are constantly being tried as guesses.	√	√	√	√	√
8	Persistent danger from within.	√	√	√	√	√
9	Constantly reiterating assaults.	√	√	√	√	√
10	Attempts to fake servers continue to occur.	X	X	√	√	√
11	standing denial of service attacks	X	X	X	√	√
12	User anonymity	√	√	√	√	√
13	Standing user impersonation attacks	√	X	√	√	√
14	Standing the leakage of short-term secret attacks	√	X	√	X	√

scheme's security weaknesses and inefficient parameters [63]. To counteract these problems, a lightweight authentication protocol has been developed for use in wireless sensor networks. This protocol enables mutual authentication, user anonymity, energy efficiency, and simple password updates. The lack of assurance of user privacy and three-factor authentication was proven in 2017 by Chaturvedi et al. [66]. It also suffered from episodes of temporary factor loss. In response, Chaturvedi et al. proposed a privacy-preserving authentication technique that makes use of biometrics to ensure user anonymity while still providing protection against active and passive attacks. In 2018, Das et al. [67] created

an efficient authentication technique for wireless sensor networks using lightweight cryptographic primitives. In 2019, Gope et al. [68] developed a forward-secure authentication system that protects users' personal information while just requiring basic cryptographic knowledge and no secret parameters.
In the year 2020, Bian et al. [69] developed a mutual authentication system based on a physically unclonable function (PUF) by combining the results of a fuzzy extractor with fingerprint biometrics.

3. Methods: Authentication without a password

Password-less authentication is a method of authenticating a computer user's identity without requiring them to reveal a password or other secret knowledge. This verification makes use of a private and public key pair. A biometric signature, hardware token, or other element that doesn't require a password is used to gain access to the public key supplied by the authenticating service (a remote server, software application, or website) upon registration. Typically, users are required to enter a username, phone number, email address, or other form of registered identification. They then have to use a standard method to establish their identity. These factors classically fall into two categories: An OTP token, smart card, hardware token, or mobile phone are all examples of "Something the user has," or possession considerations.
Fingerprints, retina scans, facial or voice recognition, and other biometrics all fall under the category of "Something the user is," or inherence criterion.
The Encryption models for fingerprint Authentication: Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA), Elliptic Curve Cryptography (ECC), RSA (Rivest-Shamir-Adleman), Homomorphic Encryption.
Some designs may utilize a mix of geo-location, network address, behavioral patterns, and gestures in place of memorized passwords.
Password-less authentication is a method of authenticating a user's identity on a computer system that does not rely on the use of a password or other knowledge-based secret. A private-public key pair is used in this technique. When you sign up for an authenticating service, such as a remote server, software, or website, that service will provide you its public key. This public key is encrypted by a private key, making access possible only with a biometric signature, hardware token, or other element that doesn't require a password. Usernames, phone numbers, email addresses, and other forms of registered identity are encouraged in common implementations. Proof of identification with an accepted authentication technique completes the authentication procedure. Location data, IP addresses, patterns of activity, and even physical movement are all included into certain designs. Password less authentication is different from MFA, even though both use multiple authentication factors. MFA provides another degree of protection to password-based authentication, but password less authentication uses a secure factor for faster and more efficient identity authentication. When all techniques are used, "password less MFA" is used to create a password less authentication flow that combines numerous variables for high security.
Computer scientists have long debated password obliteration. Famous people and experts doubt passwords can protect important data. Password less authentication is developing due to technology and corporate cultural changes. Many tech businesses and industry organizations are implementing enhanced designs and procedures to promote its adoption, including keeping passwords for specified use cases. With features like Windows Hello combining open standards like FIDO2 and WebAuthn, password less solutions have grown in popularity. Apple Safari added Face ID and Touch ID as WebAuthn platform authenticators for password less login.

3.1 Working mechanism

In order for the system to verify the identity of its users, registration is required. These are the typical procedures involved in registering without a password: [70]. When a user creates an account on a website, the server will send the user's device a "registration request." The user's device performs the authentication process after receiving the registration request (Selection of Authentication Factors 2). For security purposes, the device might scan a user's fingerprint or employ facial recognition [71]. Third, keys are generated, with the private key remaining on the user's device while the public key is sent to the server [72]. After registering, users can log in as follows:

- Authentication Challenge: The user's device receives an authentication challenge from the server [73].
- User Authentication: The user's private key is unlocked by the biometric scanner [74].
- Challenge Response: Using the user's private key, the device digitally signs the authentication challenge response [75].
- Response Validation: Using the public key on the device, the server authenticates the digital signature and grants account access [76].

Digital certificates are like password less login technology. Personal and public cryptographic key pairs are used. Consider the public key a padlock and the private key its key. Keys are unique to padlocks, and vice versa. Smartphone apps and plugin extensions help users construct a public-private key pair for safe accounts. A breakdown of the steps:

- The user's local computer stores private keys linked to a PIN, fingerprint, or facial recognition.
- The user's login website receives the public key.

Security, brand power, and efficiency in the use of IT are all boosted by passwordless authentication. Phishing, keylogging, password spraying, and brute force assaults are all ways in which hackers might get around single sign-on (SSO) and traditional multi-factor authentication (MFA). By Complete Survey all top-Notch Research Papers on Paswordless Authentication to identified the following objectives.

- Low-friction authentication improves security.
- Low-friction authentication reduces administrative costs and effort.
- Password less authentication is considered the most user-friendly.
- Deployment issues are the biggest barrier to password less authentication.
- Modern identity management platforms can considerably reduce installation challenges by integrating identity standards like FIDO and SAML.

The biggest benefit of password less authentication solutions is improved user experiences. These solutions boost labour productivity, corporate agility, and user happiness by reducing user effort, which helps retain valued people. Additionally, password less authentication can significantly reduce administrative expenses and effort. EMA responders consistently said biometric authentication and hardware tokens boost end-user productivity the most. These technologies also provided the highest security, showing a clear relationship between friction and security. Password less authentication includes password-free identity verification solutions. Physical security keys, dedicated apps, email magic links, and biometrics are password less authentication methods. While password less authentication methods vary, they all allow users to log in without a set password. Password less logins minimize friction, improve security, and improve the user experience. Businesses and industries use password less authentication. Some companies use physical security keys to protect insecure digital assets, while some online retailers offer fingerprint verification on mobile purchases. However, password less authentication goes beyond these methods and use cases and includes many implementations with different features and benefits.

3.2 Passwords weak in authentication

Password-based authentication is vulnerable to attacks that exploit the user, the weakest link in security. Reusing passwords across many services or choosing insecure options is inevitable. They may even give their passwords to phishers. Stolen credentials account for 80% of successful intrusions, with few breaches caused by system weaknesses.
Password less authentication addresses password issues. No method can guarantee account security, yet passwords alone are outmoded, forcing the development of add-ons. Multi-factor authentication (MFA) is sometimes used alongside passwords to improve credential-based authentication. These extra steps complicate the procedure and add steps for password-required users.

3.3 Types of passwordless authentication

Password less authentication has been used for decades, but new technologies are changing the identity market. The growing use of TPM (Total Platform Module) standards allows certificate-based authentication across many systems with minimal user effort which is shown in below figure 2. There is a disagreement about the legitimacy of all "password less" vendor techniques. Some solutions offer biometric authentication but only add it to a password-based architecture without FIDO2 standards. Unfortunately, hackers can intercept user data using this method. The industry agrees that just three approaches are "password less." Three main password less authentication mechanisms exist:

- Biometric authentication like fingerprints, faces, and voiceprints.
- YubiKey-style hardware security tokens.
- Certificate-based authentication.

While not incorrect, the second tier of password less authentication mechanisms is sometimes criticized for eliminating

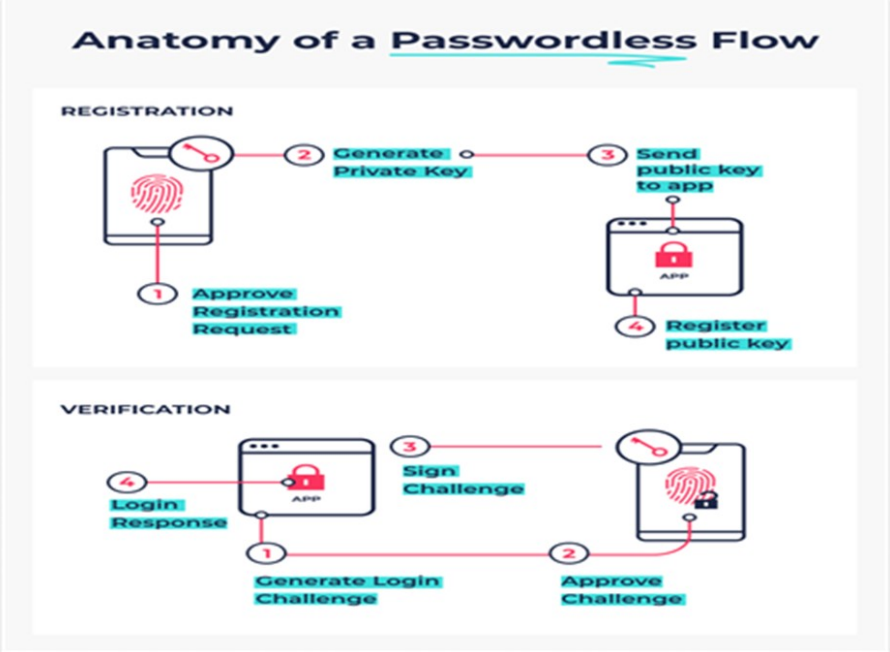

Figure 2. Password less flow chart.

passwords. Methods include:

- ▶ OTPs or PINs.
- ▶ Magic email links.
- ▶ Authenticator applications.

Email-based verification techniques cannot promise passwordlessness because most email services require passwords. Email OTPs are pseudo-passwords that use a weaker password for initial access, which limits them. SMS OTPs are vulnerable to SIM swap attacks, allowing hackers to divert text messages to their own smartphones.
Magic links face a similar problem. Despite their ease, they require passwords for authentication. The URL is accessible to everyone with an email account, so passwords are still involved.
Authenticator apps with dynamic OTPs or PINs are more secure than email. They don't eliminate passwords. Malware, man-in-the-middle attacks, and physical theft can undermine an authenticator app's device security. Attackers target the authenticator device since there is no intrinsic link between the person and the account.
User Registration

- A fingerprint reader verifies a notice of registration permission sent to the user's device when they sign up for a service or app.
- Private keys that are unique to each user are made.
- The public key is sent to the app or service.
- The public key is saved, and the private key is the only way to open it. User verification:
- The user's device gets a task when they log in.
- To accept the challenge, the user uses their biometric reader to open the private key.
- The challenge is securely signed by the private key.
- The user can log in because the public key checks the secret key.

The user's private key keeps the service provider from seeing it in true password less authentication. Biometric information is saved on the device and is only used to get to the private key.

3.4 Benefits of password less authentication

The biggest benefits of password less authentication are customer experience and security. Its benefits depend on the organization's needs. A major customer-focused organization can improve the customer experience and grow their zero-trust policy best by using a FIDO2-certified password less solution.

- ▶ Enhanced Customer Experience

Customers have an easier time using password-less authentication than standard passwords because it doesn't require them. By not having to make and remember complicated passwords, they can quickly prove who they are and shop without worrying about getting locked out. The Wall Street Journal's "Tech That Will Change Your Life in 2022" story talked about our research. It found that biometrics and choices without a password make people 44% and 35% more likely to sign up for a service, respectively.

- ▶ Increased Revenue via Reduced Customer Attrition

Mastercard reports that a third of clients abandon shopping carts due to forgotten passwords. A lower desertion rate means organizations recoup income and avoid costs. An easier, mobile-friendly identity authentication experience keeps customers coming back and boosts business growth.

- ▶ Increased Security, Password Threat Elimination

On the other hand, hackers can't get past sensors that don't require a password. They can't hack or steal biometric information and get a business to accept it. Local biometric storage on a user's device and FIDO2-based systems that use cryptographic key pairs that can't be broken into offer the highest level of security. Fraudsters use the same login for multiple services in "credential stuffing" attacks, so stolen passwords from other accounts don't work

- ▶ Sustained Cost Savings Through Reduced TCO and Infrastructure Streamlining [13]

Password-based authentication systems require IT support and maintenance, which is costly. Resetting user accounts and automating account recovery, operating call centers, and maintaining support ticketing systems require significant resources. For large companies, password support can cost millions annually. By removing passwords, large corporations can save tens of millions over time.

- ▶ Complexity in the Identity Framework was greatly reduced, making component addition and management easier.

The complexity of password-based authentication security frustrates CISOs and IT teams. Many firms use gradual, piece-by-piece identification framework augmentation as security standards evolve. This creates complicated and difficult-to-maintain authentication systems. Password less solutions simplify multi-factor authentication (MFA) implementation and regulatory compliance, requiring fewer components to provide the same security.

3.5 Applications of passwordless in IoT

Passwordless authentication in the IoT (Internet of Things) improves security and the user experience in networked contexts.

- Secure Access Control:
  IoT devices are protected from illegal access using passwordless authentication.
- Secure Biometrics:
  Biometric authentication for IoT devices, such as fingerprint or facial recognition, reduces the danger of unwanted access.

- Providing and Onboarding Devices:
  Passwordless approaches facilitate IoT device provisioning and network onboarding. Cryptographic keys can create confidence without passwords.
- Monitoring and managing remotely:
  Passwordless authentication protects remote IoT device monitoring and management by allowing only authorized users to access and operate devices.

3.6 Password less authentication vs. MFA

MFA requires two or more factors. This usually involves a password and a one-time passcode from an authenticator software, either by SMS or email which is shown in below figure 3. The number of factors used to validate a user's identification is called MFA. A fingerprint-unlocking mobile device is single-factor, yet it's password less and more secure than a password.

Multi-factor authentication is used in many password less solutions to prevent threat actors from stealing and using a device. MFA, without disrupting the user experience, commonly uses device fingerprinting as an undetectable second factor to authenticate only registered devices. The combination of biometrics and device fingerprinting makes hacker impersonation practically impossible.

The second factor may confuse users with password less MFA. FIDO2 authenticator services employ the user's device's private key as the second factor. FIDO2 uses biometric authentication and device fingerprinting to verify the private key.

Other devices can be trusted to authenticate the same user. This doesn't mean unregistered devices can log in. Security is much higher with this layered approach than with just MFA. Even if hackers beat biometric verification, they must bypass device fingerprinting, which most cybercriminals consider pointless. Bypasses have not been recorded successfully.

3.7 Benefits and limitations

While the advantages of low-friction authentication are becoming increasingly apparent, concerns about the challenges of putting these solutions into practice remain the main barriers to the widespread use of passwordless systems. To put it simply, a lot of companies are reluctant to adopt password less authentication if they expect challenges with implementation or interruptions to their business operations. Features that correspond with the "Four Features" of password less authentication are included in the most effective solutions:

- User-Friendly:
  Solutions should be easy to manage and require little administrative time for support. They should also provide a smooth onboarding experience that requires little to no end-user training.
- Perceptive:
  Entire identity ecosystem visibility should make it easier to gather contextual information about people, things, networks, and services that are hosted. Information reports have to be simple to read and comprehend, making it easier to spot possible dangers or issues with user experiences.
- Intuitive:
  By employing sophisticated technologies such as artificial intelligence, natural language processing, and analytics, gathered identity information ought to assess the degree of risk involved in authorizing entry. Depending on the amount of risk that has been determined, the user should be presented with an adaptive number of authentication factors.
- Interconnected:
  To facilitate a smooth transition between hosted services and authentication technologies, solutions should make use of industry standards like FIDO, SAML, and Open ID Connect. Access policy administration should be consolidated and administrative chores further streamlined through direct integration with platforms for system, service, and security management.
  Proponents point out a number of notable benefits over alternative authentication techniques, including:
- Better security:
  Passwords are a known weakness in computer systems that are easily broken through sharing, breaking, reusing, and spraying. They are a popular way for hackers to get in and are responsible for many security holes.
- Enhanced User Experience:
  Individuals are relieved from the burden of recalling

Figure 3. Passwordless Authentication Vs MFA.

intricate passwords or adhering to diverse security protocols. Additionally, there is no periodic requirement for them to change their credentials.

- Reduced IT Expenditures:
  In the absence of password storage and administration, IT personnel are not tasked with the responsibility of establishing password policies, detecting breaches, retrieving lost passwords, or ensuring compliance with suggested password storage practices.

- Increased Visibility of Credential Use:
  By tying credentials to particular hardware or personal characteristics, access control is tightened and the risk of widespread exploitation is reduced.

- Scalability:
  It is possible to handle several logins without making users feel tired of their passwords or requiring complicated registration procedures. On the other hand, some draw attention to operational and financial drawbacks.

- Implementation Expenses:
  While passwordless authentication may ultimately result in cost savings, the initial investments required for deployment may deter a significant number of prospective clients. The aforementioned expenses arise from the necessity to incorporate an authentication mechanism into a pre-existing user directory and, at times, from the provision of supplementary hardware to users, such as security tokens or one-time passwords.

- Requirements for Training and Expertise:
  Passwordless verification necessitates adaptation from IT teams as well as end users, in contrast to traditional password organization systems that are similar and have been around for a while.

- Dependency on a Single Component:
  When OTP or push notifications are implemented in mobile applications, end users may have difficulties in the event that their device is misplaced, damaged, stolen, or updated [77].

4. Results and discussion: Full picture of password-based and password-less authentication methods

The comparison of traditional authentication which is shown in below Table 2.

5. Discussion of new authentication methods

- Based on risk Verification (Adaptive Authentication):
  Adaptive authentication, which is also called risk-based authentication, looks at outside factors like behavior and environment during the authentication process. These factors are often used to figure out how likely it is that someone will try to log in. Based on how a user answers certain questions, the risk level determines whether they need to go through a second authentication method or be allowed to access right away. Because of this, this method of authentication is now often called risk-based authentication.

- Authentication via certificates:
  Certificate-based authentication uses digital certificates to validate the identification of individuals, computers, and other devices. A digital certificate resembles a real-world identification document, such as a passport or driver's license. This credential includes a certifying body's digital signature as well as the user's digital identification, such as a public key. Only a certifying authority may issue digital certificates as proof of public key possession. Users must show their digital certificates in order to obtain access to a server.

Future work

Future research can focus on extending the proposed password-less authentication protocol to support dynamic IoT environments with heterogeneous devices and varying network conditions. Incorporating machine learning models for anomaly detection can further enhance security against emerging threats. The integration of blockchain technology could be explored to ensure decentralized identity management and tamper-proof authentication logs. Optimization of the Artificial Hummingbird algorithm for energy-constrained IoT devices remains a key area. Moreover, a detailed performance analysis under real-time IoT deployments across domains like smart healthcare, finance, and smart cities will validate the protocol's scalability. Cross-platform compatibility and interoperability with existing identity frameworks such as FIDO2 can be studied. Enhancing resistance to side-channel and quantum attacks will also be vital. Future work may involve user behavior analysis to personalize authentication mechanisms while preserving privacy. Lastly, formal security verification through automated tools will be essential to ensure robustness before large-scale deployment.

6. Conclusion

Password-less authentication presents a promising solution to overcome traditional authentication flaws, particularly in IoT environments. The literature indicates that integrating the Artificial Hummingbird Algorithm with Modified Elliptic Curve Cryptography (MECC) offers improved performance in terms of speed, security, and efficiency. The proposed signature model demonstrates reduced signature size and faster verification, critical for real-time applications. Security is further reinforced by embedding secret keys within a Trusted Platform Module (TPM), enhancing privacy and resistance to key compromise. By leveraging the ElGamal cryptosystem within the MECC framework, the protocol achieves strong cryptographic strength. This architecture ensures lightweight, scalable, and secure authentication for constrained IoT devices. The proposed approach is well-suited for future deployment in domains such as IT, finance, and telecommunications. With ongoing enhancements, this password-less model may serve as a foundational standard for secure identity management in emerging IoT ecosystems.

Table 2. The following Authentication Type table is gives complete picture on password vs. Password less Authentication models.

authentication type	description	user productivity improvement	security effectiveness	reference
password	A memorized string of characters consisting of letters, numbers, and/or symbols that is entered when prompted to enable access.	very low	very low	[56, 78–80]
Personal Identification Number (PIN)	A short sequence of numbers (typically four to six characters) users memorize and enter when prompted to enable access.	low	low	[58, 78]
one-time passwords	Confirms users by delivering to a verified user's device or email address a password that is only valid for a single login session.	medium	medium	[58]
device authentication	Allows users that have been positively identified on a personal device (such as a PC or mobile device) to gain access to approved IT services without the need to reauthenticate.	medium	medium	[58]
hardware tokens	A physical device (such as a key fob, USB key, or smartcard) that provides an automatically generated encrypted key that substitutes traditional passwords.	medium	high	[58]
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.	medium	high	[58]
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.	medium	high	[58, 80]
behavioral biometrics	Identifies users by monitoring their uniquely applied actions and mannerisms.	high	high	[24, 57, 64]
retinal scan	A biometric technology that identifies users by scanning the unique patterns of a person's retina blood vessels.	high	very high	[24, 58]
fingerprint	A biometric technology that identifies users by reading the friction ridges of the user's thumb or other finger.	high	very high	[25]
facial recognition	A biometric technology that identifies users by their unique facial textures and shape.	very high	very high	[58]

Authors contributions
Authors have contributed equally in preparing and writing the manuscript.

Availability of data and materials
The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflict of interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. "**The quest to replace passwords: A framework for comparative evaluation of web authentication schemes**.". *IEEE S&P*, 2012.
DOI: https://doi.org/10.1109/SP.2012.44.

[2] T. Hunt. "**Passwords evolved: Authentication guidance for the modern era**.". 2020. URL https://web.archive.org/web/20200501185526/.

[3] T. Zaw and R. Yew. "**Verizon data breach investigations report (DBIR) from the perspective of exterior security perimeter**.". *Verizon Media Platform*, 2017. URL https://web.archive.org/web/20200409012027/.

[4] D. Chakraborty and S. Bugiel. "**simFIDO: FIDO2 user authentication with simTPM**.". *CCS*, 2019.
DOI: https://doi.org/10.1145/3319535.3363258.

[5] L. Bauer, C. Bravo-Lillo, E. Fragkaki, and W. Melicher. "**A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality**.". *DIM*, 2013.
DOI: https://doi.org/10.1145/2517881.2517886.

[6] S. T. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov. "**What makes users refuse web single sign-on? An empirical investigation of OpenID**.". *SOUPS*, 2011.
DOI: https://doi.org/10.1145/2078827.2078833.

[7] "**W3C**.". *Web Authentication*, 2019. URL https://www.w3.org/TR/webauthn/.

[8] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons. "**A usability study of five two-factor authentication methods**.". *SOUPS*, 2019.

[9] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides. "**Biometric authentication on iPhone and android: Usability, perceptions, and influences on adoption**.". *USEC*, 2015.
DOI: https://doi.org/10.14722/usec.2015.23003.

[10] J. Tan, L. Bauer, N. Christin, and L. F. Cranor. "**Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements**.". *CCS*, 2020.
DOI: https://doi.org/10.1145/3372297.3417882.

[11] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek. "**A comprehensive quality evaluation of security and privacy advice on the web**.". *USENIX Security*, 2020.

[12] S. Raman. "**Guide to web authentication**.". 2021. URL https://webauthn.guide.

[13] E. M. Redmiles, S. Kross, and M. L. Mazurek. "**How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples**.". *IEEE S&P*, 2019.
DOI: https://doi.org/10.1109/SP.2019.00014.

[14] E. M. Redmiles, M. L. Mazurek, and J. P. Dickerson. "**Dancing pigs or externalities? Measuring the rationality of security decisions**.". *EC*, 2018.
DOI: https://doi.org/10.1145/3219166.3219185.

[15] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons. "**A tale of two studies: The best and worst of YubiKey usability**.". *IEEE S&P*, 2018.
DOI: https://doi.org/10.1109/SP.2018.00067.

[16] Yubico. "**User presence vs. user verification**.". 2021. URL https://web.archive.org/web/20210605113506/.

[17] J. Cohen. "**A coefficient of agreement for nominal scales**.". *Educational and Psychological Measurement*, 20(1):37–46, 1960.
DOI: https://doi.org/10.1177/001316446002000104.

[18] N. Mooney. "**Addition of a network transport**.". 2020. URL https://github.com/w3c/webauthn/issues/1381.

[19] W. Oogami, H. Gomi, S. Yamaguchi, S. Yamanaka, and T. Higurashi. "**Poster: Observation study on usability challenges for fingerprint authentication using WebAuthn-enabled android smartphones**.". *SOUPS Posters*, 2020.

[20] H. Gomi, B. Leddy, and D. H. Saxe. "**Recommended account recovery practices for FIDO relying parties**.". *FIDO Alliance*, 2019. URL https://web.archive.org/web/20210520070746/.

[21] R. Kennedy, S. Clifford, T. Burleigh, R. Jewell, and P. Waggoner. "**The shape of and solutions to the MTurk quality crisis**.". *SSRN*, 2018.
DOI: https://doi.org/10.2139/ssrn.3272468. URL https://www.ssrn.com/abstract=3272468.

[22] E. Klieme, J. Wilke, N. van Dornick, and C. Meinel. "**FIDOnuous: A FIDO2/WebAuthn extension to support continuous web authentication**.". *TrustCom*, 2020.
DOI: https://doi.org/10.1109/TrustCom50675.2020.00254.

[23] D. Chakraborty, L. Hanzlik, and S. Bugiel. "**simTPM: User-centric TPM for mobile devices**.". *USENIX Security*, 2019.

[24] R. S. Chowhan and R. Tanwar. "**Password-less authentication: Methods for user verification and identification to login securely over remote sites**.". *Machine Learning and Cognitive Science Applications in Cyber Security, IGI Global*, pages 190–212, 2019.
DOI: https://doi.org/10.4018/978-1-5225-8100-0.ch008.

[25] O. Ogbanufe and D. J. Kim. "**Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment**.". *Decision Support Systems*, 106:1–14, 2018.
DOI: https://doi.org/10.1016/j.dss.2017.11.003.

[26] P. Gope and B. Sikdar. "**Lightweight and privacy-preserving two-factorauthentication scheme for IoT devices**.". *IEEE Internet Things J.*, 6(1):580–589, 2019.
DOI: https://doi.org/10.1109/JIOT.2018.2846299.

[27] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha. "**Lightweight authentication and key agreement for smart metering in smart energy networks**.". *IEEE Trans. Smart Grid*, 10(4):4349–4359, 2019.
DOI: https://doi.org/10.1109/TSG.2018.2857558.

[28] B. Ying and A. Nayak. "**Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography**.". *J. Netw. Comput. Appl.*, 131:66–74, 2019.
DOI: https://doi.org/10.1016/j.jnca.2019.01.017.

[29] M. N. Aman, S. Taneja, B. Sikdar, K. C. Chua, and M. Alioto. "**Token-based security for the Internet of Things with dynamic energyquality tradeoff**.". *IEEE Internet Things J.*, 6(2):2843–2859, 2019.
DOI: https://doi.org/10.1109/JIOT.2018.2875472.

[30] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo. "**Secure remote user authenticated key establishment protocol for smart home environment**.". *IEEE Trans. Dependable Secure Comput.*, 17 (2):391–406, 2020.
DOI: https://doi.org/10.1109/TDSC.2017.2764083.

[31] D. He, S. Zeadally, N. Kumar, and J. H. Lee. "**Anonymous authentication for wireless body area networks with provable security**.". *IEEE Syst. J.*, 11(4):2590–2601, 2017.
DOI: https://doi.org/10.1109/JSYST.2016.2544805.

[32] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang. "**Cloudaided lightweight certificateless authentication protocol with anonymity for wireless body area networks**.". *J. Netw. Comput. Appl.*, 106:117–123, 2018.
DOI: https://doi.org/10.1016/j.jnca.2018.01.003.

[33] C. Wang, Y. Zhang, X. Chen, K. Liang, and Z. Wang. "**SDN-based handover authentication scheme for mobile edge computing in cyberphysical systems**.". *IEEE Internet Things J.*, 6(5):8692–8701, 2019.
DOI: https://doi.org/10.1109/JIOT.2019.2922979.

[34] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang. "**Blockchainbased decentralized authentication modeling scheme in edge and IoT environment**.". *IEEE Internet Things J.*, 8 (4):2116–2123, 2021.
DOI: https://doi.org/10.1109/JIOT.2020.3037733.

[35] J. Wang, L. Wu, K. K. R. Choo, and D. He. "**Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure**.". *IEEE Trans. Ind. Informat.*, 16 (3):1984–1992, 2020.
DOI: https://doi.org/10.1109/TII.2019.2936278.

[36] Y. Yao, X. Chang, J. Misic, V. B. Miši´c, and L. Li. "**BLA: Blockchainassisted lightweight anonymous authentication for distributed vehicular fog services**.". *IEEE Internet Things J.*, 6(2): 3775–3784, 2019.
DOI: https://doi.org/10.1109/JIOT.2019.2892009.

[37] X. Xu, Q. Huang, X. Yin, M. Abbasi, M. R. Khosravi, and L. Qi. "**Intelligent offloading for collaborative smart city services in edge computing**.". *IEEE Internet Things J.*, 7(9):7919–7927, 2020.
DOI: https://doi.org/10.1109/JIOT.2020.3000871.

[38] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K. K. R. Choo. "**A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments**.". *J. Netw. Comput. Appl.*, 103:194–204, 2018.
DOI: https://doi.org/10.1016/j.jnca.2017.07.001.

[39] K. Jawad, K. Mansoor, A. F. Baig, A. Ghani, and A. Naseem. "**An improved three-factor anonymous authentication protocol for WSNsbased IoT system using symmetric cryptography**.". *Int. Conf. Commun. Technol.*, page 53–59, 2019.
DOI: https://doi.org/10.1109/COMTECH.2019.8737799.

[40] Y. Wen, F. Zhang, H. Wang, Z. Gong, Y. Miao, and Y. Deng. "**A new secret handshake scheme with multi-symptom intersection for mobile healthcare social networks**.". *Inf. Sci.*, 520:142–154, 2020.
DOI: https://doi.org/10.1016/j.ins.2020.02.007.

[41] J. Li, N. Zhang, J. Ni, J. Chen, and R. Du. "**Secure and lightweight authentication with key agreement for smart wearable systems**.". *IEEE Internet Things J.*, 7(8):7334–7344, 2020.
DOI: https://doi.org/10.1109/JIOT.2020.2984618.

[42] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu. "**A flexible and lightweight group authentication scheme**.". *IEEE Internet Things J.*, 7(10):10277–10287, 2020.
DOI: https://doi.org/10.1109/JIOT.2020.3004300.

[43] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun. "**A lightweight multilayer authentication protocol for wireless body area networks**.". *Future Gener. Comput. Syst.*, 78:956–963, 2018.
DOI: https://doi.org/10.1016/j.future.2016.11.033.

[44] K. Kluczniak, J. Wang, X. Chen, and M. Kutyłowski. "**Multi-device anonymous authentication**.". *Int. J. Inf. Security*, 18(2):181–197, 2019.
DOI: https://doi.org/10.1007/s10207-018-0406-4.

[45] Y. Gong, Y. Cai, Y. Guo, and Y. Fang. "**A privacy-preserving scheme for incentive-based demand response in the smart grid**.". *IEEE Trans. Smart Grid*, 7(3):1304–1313, 2016.
DOI: https://doi.org/10.1109/TSG.2015.2412091.

[46] Z. Guan et al. "**Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities**.". *IEEE Commun. Mag.*, 56(7):82–88, 2018.
DOI: https://doi.org/10.1109/MCOM.2018.1700401.

[47] C. Y. Li, X. B. Chen, Y. L. Chen, Y. Y. Hou, and J. Li. "**A new latticebased signature scheme in post-quantum blockchain network**.". *IEEE Access*, 7:2026–2033, 2019.
DOI: https://doi.org/10.1109/ACCESS.2018.2886554.

[48] E. Alkim, P. S. Barreto, N. Bindel, J. Kramer, P. Longa, and J. E. Ricardini. "**The lattice-based digital signature scheme qTESLA**.". *Int. Conf. Appl. Cryptogr. Netw. Security*, page 441–460, 2020.
DOI: https://doi.org/10.1007/978-3-030-57808-4_22.

[49] R. Ma, J. Cao, D. Feng, and H. Li. "**LAA: Lattice-based access authentication scheme for IoT in space information networks**.". *IEEE Internet Things J.*, 7(4):2791–2805, 2020.
DOI: https://doi.org/10.1109/JIOT.2019.2962553.

[50] S. Jegadeesan et al. "**An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications**.". *Sustain. Cities Soc.*, 49, 2019.
DOI: https://doi.org/10.1016/j.scs.2019.101522.

[51] V. K. Kapu and G. R. Karri. "**Efficient detection and mitigation of rushing attacks in vanets using raid: A novel intrusion detection system**.". 2023.
DOI: https://doi.org/10.3844/jcssp.2023.1143.1159.

[52] K. Vamshi Krishna and K. Ganesh Reddy. "**Classification of distributed denial of service attacks in vanet: A survey**.". *Wireless Personal Communications*, 132(2):933–964, 2023.
DOI: https://doi.org/10.1007/s11277-023-10643-6.

[53] K. V. Krishna and K. G. Reddy. "**VANET vulnerabilities classification and countermeasures: A review**.". *Majlesi Journal of Electrical Engineering*, 16(3):63–83, 2022.
DOI: https://doi.org/10.30486/mjee.2022.696508.

[54] K. Shaik and M. A. Hussain. "**Broadcast message authentication mechanism to detect clone and sybil attacks in VANET's based on ID-based signature scheme**.". *International Journal of Engineering & Technology*, 2018.
DOI: https://doi.org/10.14419/ijet.v7i3.12.17770.

[55] Shaik, Kareemulla, Md Ali Hussain, and Guntur District KLEF. "**A Novel Integrity verification based privacy preserving model for real-time VANET networks against malicious attacks**.".
DOI: https://doi.org/10.14419/ijet.v7i3.12.17770.

[56] J. Bonneau, C. Herley, P. van Oorschot, and F. Stajano. "**Passwords and the evolution of imperfect authentication**.". *Commun. ACM*, 58(7):78–87, 2015.
DOI: https://doi.org/10.1145/2699390.

[57] H. Vallabhu and R. V. Satyanarayana. "**Biometric authentication as a service on cloud: Novel solution**.". *International Journal of Soft Computing and Engineering*, 2(4):163, 2012.
DOI: https://doi.org/D0925072412/2012©BEIESP.

[58] V. Parmar. "**A comprehensive study on passwordless authentication**.". *Proceedings of the International Conference on Sustainable Computing and Data Communication Systems (ICSCDS-2022)IEEE Xplore Part Number: CFP22AZ5-ART*, 2022.
DOI: https://doi.org/10.1109/ICSCDS53736.2022.9760934.

[59] Z. P. Zwane, T. E. Mathonsi, and S. P. Maswikaneng. "**An intelligent security model for online banking authentication**.". *2021 IST-Africa Conference (IST-Africa), IEEE*, pages 1–6, 2021.

[60] E. Grosse and M. Upadhyay. "**Authentication at scale**.". *IEEE Security & Privacy*, 11(1):15–22, 2013.
DOI: https://doi.org/10.1109/MSP.2012.162.

[61] M. Kotadia. "**Gates predicts death of the password**.". *News.cnet.com*, 2004.

[62] M. Kotadia. "**Gates predicts death of the password**.". *ZDNet.*, 2004.

[63] "**IBM reveals five innovations that will change our lives within five years**.". *IBM*, 2011.

[64] V. Matyáš and Z. Říha. "**Biometric authentication—security and usability**.". *Advanced communications and multimedia security, Springer, Boston, MA*, pages 227–239, 2002.
DOI: https://doi.org/10.1007/978-0-387-35612-9_17.

[65] M. Honan. "**Kill the password: Why a string of characters can't protect us anymore**.". *Wired*, 2012.
DOI: https://doi.org/10.1055/s-0041-102167.

[66] "**Google security exec: 'Passwords are dead'**.". *CNET*, 2004.

[67] M. Grosse, E. Upadhyay. "**Authentication at scale**.". *IEEE Security & Privacy*, 11(1):15–22, 2013.
DOI: https://doi.org/10.1109/MSP.2012.162.

[68] C. Mims. "**The password is finally dying. Here's mine**.". *Wall Street Journal*, 2014.

[69] C. Mims. "**Commentary: What I learned, and what you should know, after I published my twitter password**.". *Wall Street Journal*, 2014.

[70] "**Making authentication even easier**.". *security.googleblog.com*, 2019.

[71] "**Apple developer documentation**.". *developer.apple.com*, 2020.

[72] "**Passwordless authentication: A complete guide [2022] - transmit security**.". *Transmit Security*, 2022.

[73] "**No password for Microsoft Account: What does passwordless authentication mean?**.". *Business Today*, 2022.

[74] K. Deighton. "**Technology alliance says it is closer to killing off passwords**.". *Wall Street Journal*, 2022.

[75] "**Accelerating the journey to passwordless authentication**.". *IBM*, 2022.

[76] "**Passwordless authentication**.". *World Economic Forum*, 2022.

[77] N. Smithson. "**Issues with multi-factor authentication: PSA for MFA app users**.". *sayers.com*, 2020.

[78] S. G. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel. "**Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication**.". *IEEE Symposium on Security and Privacy*, pages 268–285, 2020.
DOI: https://doi.org/10.1109/SP40000.2020.00047.

[79] Z. P. Zwane, T. E. Mathonsi, and S. P. Maswikaneng. "**An intelligent security model for online banking authentication**.". *2021 IST-Africa Conference (IST-Africa), IEEE*, pages 1–6, 2021. URL https://ieeexplore.ieee.org/abstract/document/9576963.

[80] I. Matiushin and V. Korkhov. "**Passwordless authentication using magic link technology**.". *CEUR Workshop Proceedings, RWTH Aahen University*, 3041:434–438, 20.
DOI: https://doi.org/10.54546/MLIT.2021.89.13.001.