IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 December 2024, accepted 31 December 2024, date of publication 13 January 2025, date of current version 23 January 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3528960

SURVEY

Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity

MOHD IMRAN MD YUSOP, NAZHATUL HAFIZAH KAMARUDIN, (Member, IEEE), NUR HANIS SABRINA SUHAIMI, (Member, IEEE), AND MOHAMMAD KAMRUL HASAN, (Senior Member, IEEE)

Centre for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia

Corresponding author: Nazhatul Hafizah Kamarudin (nazhatulhafizah@ukm.edu.my)

This work was supported by Universiti Kebangsaan Malaysia (UKM) under the Research Grant Scheme under Grant GGPM 2023-070.

ABSTRACT As reliance on digital services grows, traditional password-based authentication methods have been increasingly scrutinized due to their susceptibility to cyber-attacks, including phishing and brute force attacks. This has led to a shift toward passwordless authentication, an approach that promises enhanced security and user experience. This paper provides a comprehensive review of passwordless authentication techniques, analysing their application in user identity verification across multiple platforms. Various methods such as biometrics, security keys, and token-based systems are explored for their efficacy in mitigating security vulnerabilities. The review highlights the advantages of passwordless authentication, including improved security, reduced user friction, and compatibility with modern identity management frameworks like FIDO2. Challenges such as usability issues, cost of deployment, and scalability are also discussed. Moreover, the paper identifies future research areas aimed at overcoming these challenges and facilitating the broad adoption of passwordless authentication in critical industries such as healthcare, finance, and public services. Future opportunities are outlined, emphasizing the need for real-world implementation, enhanced scalability, integration of AI-driven adaptive mechanisms, and innovative designs to improve user accessibility and system resilience. By consolidating existing knowledge and identifying gaps in current solutions, this study provides valuable insights for researchers and industry stakeholders seeking to enhance security through passwordless systems.

INDEX TERMS Authentication, biometric, FIDO, passwordless, network security, user identity.

I. INTRODUCTION

Passwords, which are text-based, remain the most widely used authentication method across various systems and applications due to their simplicity and ease of deployment. They do not require in-depth knowledge of cryptography or complex security protocols, making them accessible for both users and developers. Password-based authentication relies on the user's ability to recall a secret passphrase to verify their identity and access systems, devices, or applications. This method falls under the "something you know" category in the three-factor authentication model. However, despite its popularity, password-based authentication is plagued by several vulnerabilities, including weak or easily guessable passwords, which often lead to data breaches and unauthorized access [1]. Several studies have been conducted to improve password-based authentication such as introducing 2FA or MFA as well as using password manager. However,

The associate editor coordinating the review of this manuscript and approving it for publication was Khursheed Aurangzeb.

user experience in using 2FA and MFA has been determined to be difficult and unpleasant, further delaying the verification process [2].

Password managers have also faced security challenges, as studies have shown that passwords stored in these managers can be extracted and stolen through automated network attacks [3]. Recently, passwordless authentication has gained traction as a form of authentication that could replace password-based authentication. Passwordless authentication is basically a mechanism used for authentication that does not rely on text-based password for authentication. Passwordless uses authentication such as biometrics, behavioural, certificate-based such as public key, tokens, physical security key, magic links and many more [4]. This authentication usually falls under what you are or what you have and have much better security features than the traditional password.

The FIDO Alliance was established to create open standards aimed at simplifying and strengthening online authentication [5]. Supported by major tech companies such as Google, Microsoft, and Apple, the Alliance introduced protocols like UAF, U2F, and FIDO2 (which includes CTAP and WebAuthn). These protocols leverage various advanced technologies to enable more secure and user-friendly authentication methods [6]. With the growing adoption of FIDO standards, the shift from traditional password-based authentication to passwordless authentication is becoming increasingly inevitable. While the FIDO Alliance has made significant strides in promoting passwordless authentication, challenges remain in achieving widespread adoption [7]. This includes usability, interoperability issues, implementation cost, and user education [8], [9], [10]. Despite these challenges, the momentum behind FIDO protocols signals a promising shift towards a more secure and user-friendly authentication landscape, paving the way for a future where passwords are no longer the primary means of user identification.

This study aims to carry out a comprehensive analysis of passwordless authentication that focuses on user identity. One of the main objectives is to assess passwordless authentication in terms of their effectiveness, security, usability, and challenges in implementing this method. By evaluating various passwordless authentication approaches, including biometrics, security keys, and token-based authentication, this review seeks to provide insights into the strengths, weaknesses, and implementation considerations of each method. Ultimately, the goal is to provide valuable insights and possible areas for future research to enhance user identification using passwordless mechanism while mitigating security risks associated with traditional password-based authentication methods. Figure 1 presents the contribution breakdown of this paper.

A. MOTIVATION

The purpose of this review is to extensively study the current implementations of authentication methods without passwords as an alternative to conventional methods in user identity identification. The main motivation behind this study are as follows:-

- Reduce cybersecurity risks associated with traditional password-based systems. Conventional methods are often vulnerable to cyber-attacks such as identity spoofing, password hacking, and weak password usage
- Investigate the effectiveness and key components of passwordless authentication solutions.
- Evaluate the benefits, challenges, and implementation domains of passwordless methods.
- Identify areas for improvement and innovation in passwordless authentication systems.
- Enhance understanding of the feasibility and potential of passwordless techniques in digital security.

TABLE 1. List of research questions.

RQ	*Research Question*	*Objectives*
RQ1	What are the domains of studies?	Determine the areas of application explored by previous research using passwordless authentication.
RQ2	What is the problem statement of the studies done?	Understand the problems addressed by previous research regarding the need of passwordless authentication or the issues faced while deploying passwordless authentication.
RQ3	What are the contributions of those studies?	Identify the advancements and improvements introduced by previous research in passwordless authentication.
RQ4	What passwordless mechanisms that have been used?	Analyse the different approaches used for passwordless authentication in previous studies.
RQ5	What are the performance metrics used?	Evaluate how previous research measured the effectiveness and efficiency of passwordless authentication methods.
RQ6	What are the attacks that can be mitigated?	Identify the security vulnerabilities addressed by passwordless authentication solutions explored in previous research.
RQ7	What is the limitation or issue of the passwordless solutions?	Recognize potential weaknesses and limitations of the existing passwordless solutions that has been proposed or tested.
RQ8	What are the potential future works?	Explore new directions and areas of investigation for further development of passwordless authentication.

B. CONTRIBUTIONS

This review paper makes several significant contributions to the ongoing discourse on user authentication and cybersecurity by addressing key challenges, consolidating insights, and exploring future possibilities in passwordless authentication. These contributions not only bridge existing gaps in the literature but also provide practical guidance for researchers, developers, and organizations aiming to adopt or improve passwordless methods. The specific contributions are as follows:

- provides a comprehensive overview of the current landscape of passwordless authentication techniques which includes its implementation domains, benefit and challenges.
- consolidates valuable insights in seeking to understand and implement passwordless authentication solutions.

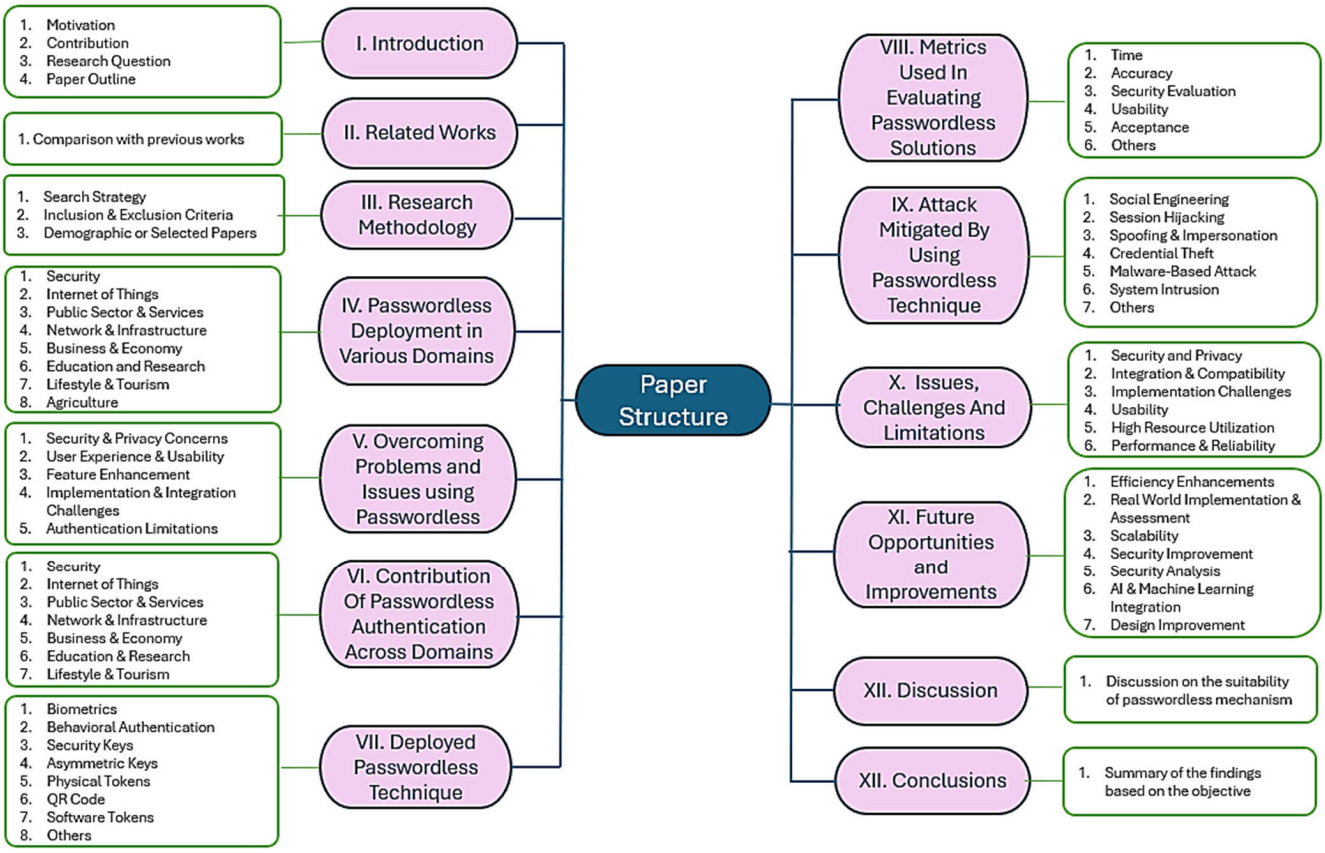


FIGURE 1. Structure of review paper.

- identifies common passwordless techniques that have been deployed and offers a comparative analysis of each passwordless solutions that has been deployed. This comparative evaluation can guide organizations and developers in selecting the most suitable password-less authentication method for their specific use case considering factors such as security requirements, user experience, and scalability.
- this review delves into the possibility of issues associated with passwordless authentication and explores viable future strategies for improvements. By highlighting areas for future works, this paper contributes to the ongoing efforts to enhance the robustness and resilience of passwordless authentication systems.

C. RESEARCH QUESTION

To achieve the objectives of this study, eight research questions have been identified, with the motivations for each detailed in TABLE 1. These questions are aimed at uncovering common themes of identified problems, contributions of each work, the authentication methods used, evaluation metrics, study limitations, and potential areas for future research.

The research questions are designed to explore the current state of passwordless authentication in user identification. This review will analyse and discuss each of these questions in detail, offering insights into the identified challenges and advancements. The structure of the paper is organized to address these questions, as outlined in FIGURE 1.

II. RELATED WORKS

Several related research has been conducted in reviewing and analysing various authentication methods. Reference [4] reviews an overall authentication method consists of traditional and password-less authentication by highlighting the advantages and disadvantages of each authentication that are available for a better understanding of each of the technology. Reference [11] conducted a comprehensive study focusing on multi-factor authentication in various platforms to identify how different multi-factor authentication systems work and what are their disadvantages. Focusing on authentication in IoT realms, [12] conducted a comprehensive analysis of authentication trends in IoT on recent developments, protocols, and security concerns in IoT. Reference [13] reviews and assess the potential of passwordless in replacing password as a modern solution to digital systems. As part of IAM requirements in enterprises and potential of SSI sovereign identity (SSI) as a passwordless paradigm in identity management, [14] study concluded that even though SSI was deemed to enhance manageability, usability, and least privilege in IAM, it is not a complete solution for all IAM challenges. A different approach taken by [2] which focuses more on passwords and modern authentication threats and recommends FIDO2

TABLE 2. Comparison of previous studies with this paper.

Papers	Point of interest	Contribution
[2]	Password and modern authentication threats	Identifies the importance of balancing security, usability, and privacy in any new authentication method.
[4]	Password and passwordless mechanism	provides a detailed review of various passwordless authentication technologies, discussing their advantages and disadvantages
[8]	analysing the obstacles in adopting FIDO password-less as a single factor authentication	Highlights the barrier of widespread adoption using FIDO as single factor due to lack of standardized procedures for account recovery, deletion, as well as issues with the usability of FIDO security keys
[10]	Survey on passwordless perception from 118 IAM professional	identifies and analyses the challenges of integrating the FIDO2 passwordless authentication system in enterprise environments that focus on issues such as account recovery, remote access, and the need for better integration guidelines
[11]	comprehensive study focusing on multi-factor authentication that include passwordless	provides a comprehensive analysis focusing on multi-factor authentication on various platform in terms of security, usability, and how they mitigate risks
[12]	Authentication trends in IoT	provides a detailed review of recent developments in authentication methods for the Internet of Things (IoT)which includes strengths and weaknesses of various protocols to help improve security and scalability in IoT systems
[13]	Passwordless in digital system	highlights security issues and potential attacks of modern authentication including multifactor, passwordless, adaptive, and continuous authentication
[14]	Passwordless in IAM and SSI	identifies and categorizes the requirements for Identity Access Management (IAM) systems in enterprises and evaluates how Self-Sovereign Identity (SSI) can meet these needs
[15]	Remote biometric authentication	Provide analysis of six different remote biometric authentication systems regarding strengths and weaknesses.
[16]	fingerprint acquisition techniques and sensor types for authentication technology	reviews latest advancements in fingerprint sensor technology, different types of sensors and their applications, highlighting their benefits and limitations for large-scale use in various industries
[17]	FIDO2 passwordless in various type of deployment	Findings shows that significant advantages of FIDO2 will not completely replace passwords due to various technical and user-related challenges
This paper	Passwordless technique and mechanism applied as single factor or multifactor for user identity in various domain and platforms	This paper distinguishes itself by offering a comprehensive and systematic analysis of passwordless authentication across diverse mechanisms, domains, and evaluation metrics that surpass the limited scope and focus area of prior works. Insights are integrated and grouped into categories from rigorous data sources and present unique perspectives based on performance metrics, deployment trends in various domains, attacks that can be mitigated, challenges, and future research opportunities. This will help in understanding critical gaps, providing a forward-looking roadmap for advancing passwordless technologies.

passwordless standard as the potential solution. This study also emphasizes the need for balancing security, usability, and privacy for modern day authentication methods.

In the field of biometrics, [15] evaluates remote biometric authentication systems as potential replacements for passwords by analysing six different remote biometric authentication implementations. A set of criteria for comparing authentication schemes was proposed to guide future biometric evaluations. In [16], the authors discuss various fingerprint acquisition techniques and sensor types used in authentication technology, highlighting the limitations of current fingerprint recognition methods and suggesting areas for future improvement. By analysing the obstacles in adopting FIDO password-less as a single factor authentication, [8], [10] highlights security, usability, enterprise requirements, and account recovery as the main issues where users and companies tend to disregard the passwordless mechanism as a choice of implementation. In the application of passwordless in various deployment, FIDO2 approach is discussed [17] and suggested that password elimination is not feasible in the near future due to its foreseen challenges.

Overall, these studies underscore the obstacles and challenges in adopting passwordless authentication. This paper builds on prior research by conducting an in-depth analysis of existing passwordless technology solutions for user identification. It examines the initial problems addressed by each study, along with their contributions and limitations, and explores potential future research areas based on recurring themes and categories. Additionally, this paper identifies the passwordless techniques and evaluation metrics currently attracting interest and being adopted by researchers. A comparison with previous studies is presented in TABLE 2.

III. RESEARCH METHODOLOGY

This section describes the methodology and approaches used in this review. The methodology used is the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) protocol [18]. The flow of this research involves

FIGURE 2. Research phas.

three main steps which includes planning phase, review phase and reporting phase as shown in FIGURE 2.

A. SEARCH STRATEGY

A total of four databases have been identified for searching related articles which are Scopus, Web of Science, ProQuest and IEEE Xplore. Papers searched consists of recent papers from 2020 until 2024. The keywords used for the search in these databases are ''passwordless'' or ''password-less'', ''FIDO'' or ''FIDO2''. Boolean operators such as ''AND'' and ''OR'' including parentheses were used to search these keywords in the databases. The keywords are searched in each database to match either the title or in abstract. A total of 569 papers were found for these databases. After reviewing the papers, a total of 128 duplicates have been removed.

B. INCLUSION AND EXCLUSION CRITERIA FOR SELECTION

In this review, the following criteria are used to filtered and select the papers that has been searched for: (1) recent papers from year 2020 until 2024 (2) the papers in English or has English version. (3) Related papers that have studied on password-less mechanism. (4) Papers are available for download. (5) and papers that have proposed in terms of design, framework, or deployment of passwordless mechanism in their studies. Papers were excluded if (1) not relevant to the topic, research question of objective of this review (2) not available in full text. (3) Papers that study on non-passwordless authentication methods, (4) papers that do not have design, framework, or deployment of passwordless mechanism in their studies. (5) Papers that not available in English. Inclusion and exclusion criteria are summarized in TABLE 3.

The overall process of selection and filtering the papers using the PRISMA statement methodology are shown as in FIGURE 3.

C. DEMOGRAPHICS OF SELECTED PAPERS

By using the PRISMA statement, this paper has identified a total of 81 papers that will be examine and rigorously vet through in understanding the status of passwordless implementation. FIGURE 4 shows the types of publications that have been selected.

IV. PASSWORDLESS DEPLOYMENT IN VARIOUS DOMAINS

Detail examination was conducted towards the nature and elements in the selected studies. The section thoroughly analyses areas that the studies focused on using password-less authentication. This paper organizes these areas into eight main domains consisting of Security, IoT, Public Sector

TABLE 3. Inclusion and exclusion criteria.

	Inclusion Criteria
IC1	The paper publishes between 2020 - 2024
IC2	The paper is written in English
IC3	Related papers that have studied on password-less mechanism
IC4	Papers are available for download
IC5	papers that have proposed in terms of design, framework, deployment of passwordless mechanism in their studies
	Exclusion Criteria
EC1	Papers that are not relevant to the topic, research question or objectives of this review.
EC2	Papers that are not available in full text
EC3	Papers that do study on non-passwordless authentication methods
EC4	papers that do not have design, framework, or deployment of passwordless mechanism in their studies
EC5	Papers that not available in English

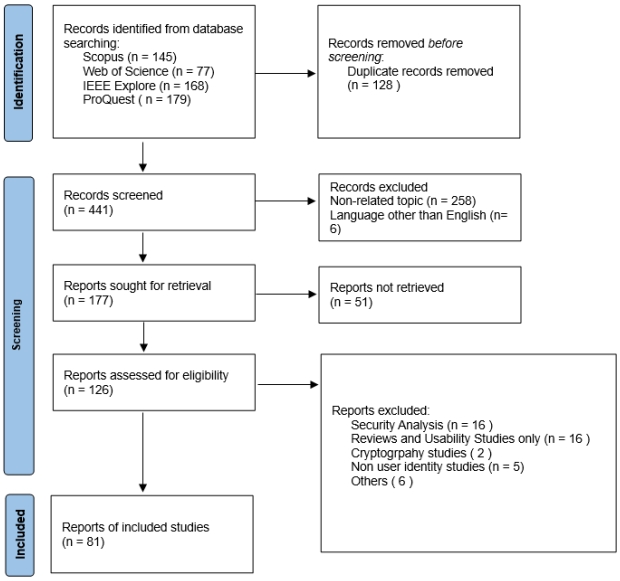


FIGURE 3. Selection flow using PRISMA methodology.

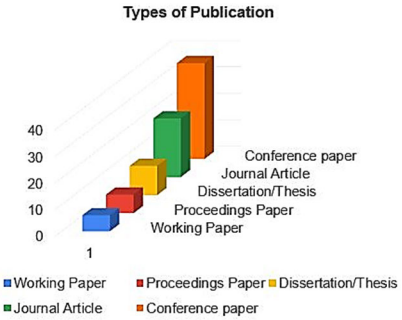


FIGURE 4. Selected publications by type.

and Services, Network and Infrastructure, Business and Economy, Education and Research, Lifestyle and Tourism and Agriculture Each domain is accompanied by a specific count of research papers and the corresponding percentage representation, providing a comprehensive overview of the research landscape as shown in FIGURE 5 and TABLE 4.

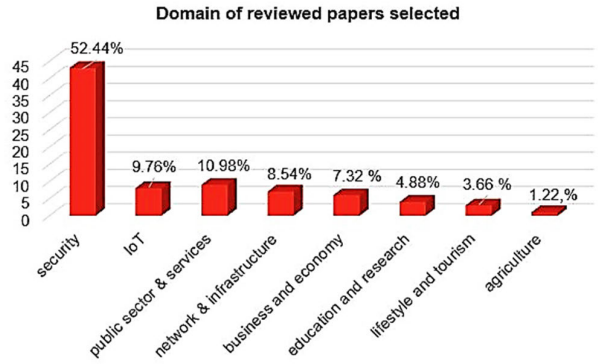


FIGURE 5. Distribution of the domain in previewed paper.

TABLE 4. Selected papers by domain.

Domain	Papers studied in this domain
Security	[19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55],[56], [57], [58], [59], [60], [61].
Internet of Things	[62], [63], [64] [65], [66] [67], [68], [69].
Public Sector and Services	[70], [71], [72], [73], [74], [75], [76], [77] , [78]
Network and Infrastructure	[79], [80], [81], [82], [83], [84], [85]
Business and Economy	[86], [87], [88] [89], [90], [91]
Education and Research	[92], [93] [94], [95]
Lifestyle and Tourism	[96], [97],[98].
Agriculture	[99]

A. SECURITY

Authentication is vital for verifying user identity to prevent unauthorized access and breaches including securing sensitive data. Most of the studies focused on the security domain which constitutes 52.44% of the selected studies. In this domain, several studies concentrate on improving authentication with the purpose of replacing passwords due to its security issues [21], [25], [30]. Researchers focuses on the inherent usability issues on multifactor authentication [29], [50] and security tokens [52], [55]. Passwordless also used as an additional layer in improving security as a second factor [33], [34], [35]. Studies in [53] and [58] address the current limitation of passwordless in terms of security aspects. Adding additional features to enhance passwordless techniques or protocols were the primary focus in studies [36], [42], [49]. In addition, studies in [56], [59], and [60] lean towards on enhancing security for online and web applications by using passwordless solutions.

B. INTERNET OF THINGS (IoT)

Authentication is essential part for users accessing IoT devices and for managing and securing interconnected devices and data networks securely. This domain consists of 9.76% of the studies with papers conduct research for passwordless authentication using smart wearables [62], [63], [64] and IoT devices [65], smart cities applications for traffic offense [66] and continuous authentication [67], and vehicles implementing IoV concepts [68], [69].

C. PUBLIC SECTOR AND SERVICES

Authenticating user identity in accessing public services requires reliable identification of citizens and users for protecting data and privacy. In this domain, studies were done on authentication to improve government applications [70], [71], electronic ID integrations [72], [73], [74], [75], healthcare [76], [77] and smart energy [78]. 10.98% of the studies represent this domain.

D. NETWORK AND INFRASTRUCTURE

In this domain, it is vital for authenticating users to control access and protect network and infrastructure integrity. Infrastructure consists of telecommunications [81], cloud [80], [82], [85], and network [79], [83], [84] are deemed to have beneficial security effect in integrating various passwordless techniques. This domain consists of 8.54%.

E. BUSINESS AND ECONOMY

In business and economy, authentication is an integral security control in protecting corporate assets and facilitating secure transactions. 7.32% of the selected studies explores the possibility of using passwordless into the business and economy domain, which use to secure digital assets [86], physical assets [87], managing commercial transactions [88] and finance institutions and transactions [89], [90], [91].

F. EDUCATION AND RESEARCH

Education and research provide resources for intellectual growth and innovation, and it is important for secure access to these educational resources and research data. The domain of Education and Research contributes to 4.88% were focusing on enhancement using passwordless for online examination [92], integration of passwordless to access research applications and data [93] and improving security in education application and sector as a whole [94], [95].

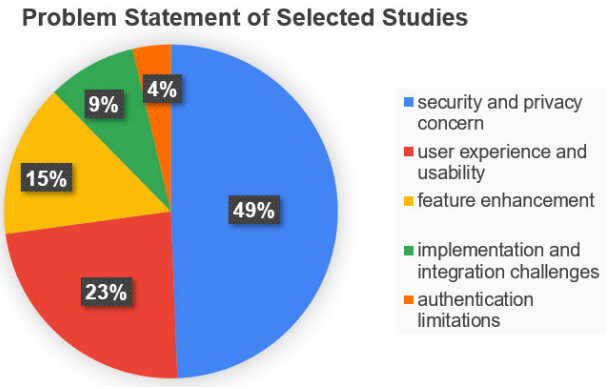


FIGURE 6. Distribution of category of problems in the previewed studies.

G. LIFESTYLE AND TOURISM

User authentication ensures secure transactions and protects personal information in leisure and travel. Comprising of 3.66% of the studies, [96], [97] applied a passwordless authentication for the usage in virtual space and for the tourism sector [98].

H. AGRICULTURE

In agriculture domain, authentication is important for verifying identities in agricultural processes and managing farm data securely. 1.12% of study represents the agriculture domain where [99] deploying a passwordless technology to help farmers authenticate for data while doing their work.

V. PROBLEMS RELATED TO PASSWORDLESS AUTHENTICATION IMPLEMENTATION

According to the selected papers that have been reviewed, there are several main problems that have been highlighted on why passwordless is selected and issues encountered on using passwordless deployment. These issues are identified and grouped into main categories by reviewing each problem statements in the selected papers as shown in FIGURE 6 and TABLE 5.

A. SECURITY AND PRIVACY CONCERNS

The most common issues are regarding the security and privacy concerns that users must dealt with when using traditional authentication methods especially using text-based passwords which prompts a requirement for a better alternative's authentication solution. This is due password remains to be exposed to multiple security issues [21], [25], [30], [80]. This method also plagued with inherent shortcomings such as insecure password practices [23], and password management issue [27]. In web applications, traditional authentication using passwords is lacking in terms of user control and privacy over identity data [61] and susceptible to phishing and malware attacks [56]. In healthcare settings, the inefficiency of current security controls across overall system access [76] necessitates real-time detection and verification of legitimate healthcare providers to mitigate scams [77].

TABLE 5. Categories of problem statements of selected papers.

Problem Statement Category	Paper
Security and privacy concerns	[19], [21], [22], [23], [25], [27], [28], [30], [31], [32], [34], [35], [36], [37], [43], [44], [45], [56], [60], [61], [65], [69], [70], [71], [72], [73], [74], [76], [77], [80], [84], [86], [87], [88], [89], [90], [94], [95], [96], [97]
User experience and usability	[20], [24], [26], [29], [33], [40], [46], [47], [48], [49], [50], [52], [54], [55], [62], [75], [78], [82], [91].
Feature enhancement	[38], [39], [41], [42], [57], [63], [64], [66], [67], [68], [81], [92]
Implementation and integration challenges	[51], [59], [79], [83], [85], [93], [98]
Authentication limitations	[53], [58], [99]

Single current password-based authentication systems provided by academic federations can lead to impersonation by attackers across all federated service providers when the password has been compromised [95]. Current systems often fail to verify the legitimacy of users when passwords are used by unauthorized parties [31], [36]. Solutions like FIDO2 struggle with post-login attacker detection [43]. Mobile money applications that rely on 2FA with PIN and SIM are vulnerable to security attacks due to insecure algorithms [89], and account losses from forgotten password recovery remain a significant concern [22]. The rise of sophisticated cyber-attacks has rendered traditional authentication methods increasingly obsolete [25], exacerbated by the centralization of public services which increases susceptibility to cyber-attacks [71].

Passwordless authentication solutions improve overall security but are not without issues. Researchers have highlighted concerns such as biometric vulnerabilities to spoofing attacks [37] and the replication of facial features from images [45]. Dynamic authentication using WiFi to detect user behaviour faces challenges in real-world scenarios like location and environmental changes [84]. For smart devices, implicit authentication is required due to security concerns [44]. Smart devices also pose new security and privacy risks because their advanced capabilities that can be exploited by attackers despite regulatory efforts to give users control [96]. Smart wearables' utilization of keystroke dynamics for authentication effectiveness in real-world applications remains uncertain and need to be further evaluated [35]. In metaverse which adopting Web 3.0 technology, a user's real-life identity is directly linked to its virtual identity and which breaches and risks in their virtual identity can be a threat to their actual identity [97]. The Internet of Vehicles (IoV) faces concerns over data leakage from side-channel attacks and key disclosure issues and thus poses significant privacy risks [69].

Furthermore, centralized Identity Providers (IdPs) introduce trust issues that necessitates mutual trust between IdPs and Service Providers (SPs) regarding user data and identity

attributes [72]. The absence of usable and secure Identity Management (IdM) solutions further jeopardizes trust in digital ecosystems [73]. Additionally, internet voting systems raise fears of election manipulation [70], traditional physical locks lack key management and access control capabilities [87], and traditional ticketing methods are vulnerable to ticket scalping activities [88].

B. USER EXPERIENCE AND USABILITY

The second issue highlighted that the usability and acceptance on moving towards passwordless authentication is considered as a barrier towards adoption and deployment. In terms of user experience, additional action for authentication deemed to be unsuitable for on-the-fly authentication [24] and giving bad user experiences when using MFA for authentication [33]. In banking sector, account opening is a time consuming and cumbersome process especially when involving multiple identity providers for user identity authentication [91]. Prevalent uses of passwords require increase security measures such complex passwords usage that lower user experience and thus require for suitable authentication methods [78]. Drawbacks such as re-registration of authenticator in different websites and services and carrying additional device for authentication is a major concern [54].

In regards of usability, [20] highlighted that usability on FIDO2 on mobile devices has not yet been studied. Practical issues of FIDO2 standards causes reluctance in adoption by service providers [26]. Some connectors such as USB interfaces for passwordless are not available on user devices [40]. Lack of user trust, habits, awareness, perceptions, concerns [46], [49], [75] and misconceptions [47] are the main problems in adopting a passwordless mechanism. New solutions in replacing passwords also grapples with usability, deployability and security complexities [48]. The emergent of hardware tokens are still not widely adopted due to its impracticality and additional effort to carry around [52], [55]. Meanwhile, although password managers and two-factor authentication offer improved security, it suffers from usability challenges [29], [50], [82].

C. FEATURES ENHANCEMENT

Subsequently, 15 % of the reviewed papers identified that some of the passwordless authentication mechanisms lack certain features in terms of functionality or capabilities that can be improved to make it more efficient. this include SIM cryptography capabilities for authentication is not fully utilized [81], large storage issue for photo-based authentication [38], level of performance when using eye movement [41], manual traffic systems issues [66], lack of the ability to mix trusted user elements for authentication in FIDO2 [42], and lack of standards and open-source solution for smart cards integration [57]. Identity monitoring for online examinations also missing a much more dependable authentication solutions [92]. For smart city, there is a minimum number of studies that focus on leveraging comprehensive set of sensors data to elevate behavioural

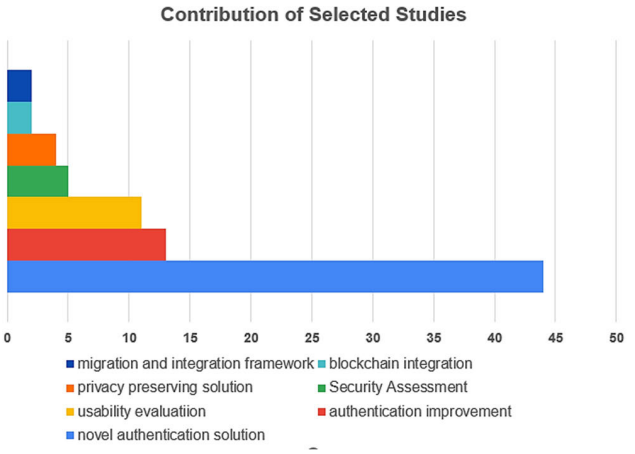


FIGURE 7. Distributions of previewed studies contributions.

authentication [67]. In terms of smart wearables, there is a need for implicit authentication features [63], [64]. In IoV, knowledge-based authentication is not suitable thus requires a more feasible features [68].

D. IMPLEMENTATION AND INTEGRATION CHALLENGES

Implementing and integrating passwordless also poses as a challenge for passwordless implementation. This includes challenges of interoperability in various interconnected devices [98], deployment for VPN environments [83], integration for network authentication [79], camera-based for 2FA challenges [51], and secure and effective cloud services authentication [85]. Multiple accounts of the same users from different providers to access multiple services that needed to be integrated that leads to inefficiency authentication [93] and complication of SSO implementation that are not compatible with some application in an enterprise environment with password as a prevalent method making passwordless implementation hard [59]. Thus, there is a need to rectify these problems to enable and provide more scalability and widespread deployment, which contributes to 9 % of the studies.

E. AUTHENTICATION LIMITATIONS

Representing 4% of the selected studies, the least problem that has been noted in papers [53], [58], [99] are due to some limitations in the passwordless mechanism.

VI. CONTRIBUTION OF PASSWORDLESS AUTHENTICATION ACROSS DOMAINS

Based on the identified problems, researchers have proposed solutions constituting integral contributions within each respective academic study. These contributions are grouped into category as shown in FIGURE 7 and mapped into its respective domain as shown in TABLE 6.

A. SECURITY

In terms of contributions, most of the previewed study in this domain studies proposed a novel authentication method

TABLE 6. Mapping of reviewed studies based on domains.

Domains	Contribution Trends						
	Novel solutions	Authentication improvement	Usability evaluation	Security assessment	Privacy preserving solution	Blockchain integration	Integration and migration framework
Security	[19],[24],[30],[31], [32],[33],[34],[35], [36],[38],[39],[41], [42],[44],[45],[48], [51],[52],[53],[56], [58],[59]	[27],[28],[37], [40],[49], [50],[57]	[20],[21],[22], [26],[29],[46], [47],[54],[55]	[22],[25], [43]		[60]	[61]
IoT	[62],[63],[64],[65], [66],[67],[69]				[68]		
Public Sector and Services	[70],[76],[77],[78]	[73],[74]	[75]		[72]	[71]	
Network and Infrastructure	[79],[81],[84],[85]	[82]		[83]			[80]
Business and Economy	[90],[91]	[86],[88],[89]		[87]			
Education and Research	[92],[94],[95]		[93]				
Lifestyle and Tourism	[97]				[96],[98]		
Agriculture	[99]						

used as a single or additional factor. Leveraging Biometrics capabilities, [19] proposed a novel multi-modal biometric system based on face and fingerprint user authentication system that converts into DNA QR code. [33] introduce a robust and secure multi-factor user authentication method called BioDraw that extracts four biometric features from a single swipe for high-security multi-factor authentication. This method consists of RFID component Development of a novel anti spoofing scheme called Binary ALOHA mechanism and a CNN-LSTM based classifier for user recognition. A new 3D password scheme was developed by [58] for real-time authentication that utilizes facial expression, eye-ball movement, and keyboard values for authentication. By using behavioural pattern as an authentication method, [24] introduces BehaviorID that incorporates A-RNN for behavioural tracking, [35] propose using keystroke dynamics in converting behavioural biometrics data into 3D images and [44] provide a solution for passive and continuous authentication via user smartphone interaction with 3 machine learning classifiers. Another novel keystroke dynamics authentication method was proposed by [78]which this solution is based on text retrieval. Several novel passwordless authentication that utilizes non-biometric were proposed, such as using magic link for online services [30], sequential or non-sequential of images selection that has been converted into strings and stored in database for easy user recognition [38] and a camera-based authentication system authentication called PhotoAuth with additional feature of detecting address bar content to counter fake domains on the browser URL bar [51]. SSI concepts were integrated with passwordless authentication for a more secure access to web applications, as [60] incorporates Hyperledger Aries for blockchain and ZKP tool that uses QR Codes and private-public keypairs for authentication while a framework with SSI for accessing restricted web services was designed [61]. In addition, [27] developed an Android-based passwordless system with Flutter framework which implements Multi-Factor Authentication (MFA) features that includes usernames, and OTP codes. Reference [52] propose Symbolon, a framework for secure user passwordless authentication with multiple devices. An end-to-end framework proposed by [42] called FIDO-AC that combines FIDO2 with digital identity solution that integrates attribute-based for authentication. [56] propose FIDO2D for secure web authentication schemes for handling security-critical transactions that fulfil the concept of one-out-of-two security. Focusing on increasing adoption by service providers and compliance with the PSD2 directives, [26] developed StrongMonkey SDK that connects to a FIDO2 server for passwordless authentication. Reference [48] introduces Let's Authenticate, an authentication which combines elements of password managers, FIDO2, and certificate. Reference [59] introduces ROSTAM that integrates credential manager and federated identity systems for SSO multifactor authentication where passwords of different services are stored and can be unlocked using a passwordless primary key. In addressing the critical challenge of two-factor authentication, [22] presented a solution through the design and implementation of a passwordless recovery authenticator. Reference [50] produce a mobile authenticator without hardware costs that leverages FIDO and Android security and integrates it into password manager solutions.

This domain also shows a common theme in enhancing passwordless with other features or improving security capabilities and efficiency. Security and privacy enhancement was the target of [36] with the introduction of an accountable authentication framework extension called Larch, that ensures every passwordless authentication attempt is recorded without revealing the web service being accessed to the log server. Focusing on iris detection mechanism enhancement, [37] added eye-liveness feature by reading pupil diameter measurement and heartbeat and [41] incorporated eye movement detection using DenseNet-based CNN model for increasing authentication performance. Addressing FIDO limitations, an extension proposed by [40] and [49] using QR Codes, where the former facilitate a more secure authentication flow while the latter adopts QR codes for message transmission to remove hardware requirements during registration and authentication of external authenticators. Due to the lack of FIDO passkey management feature, a novel extension for multiple passkey management and synchronization was designed [53]. Enhancing the usage of phone as an authenticator was introduced by [39] via a solution called homomorphic encryption-based device owner equality verification (HE-DOEV), which helps verifying a user is the same person owns two different devices without sharing any private information like personal details or long-term identifiers. Reference [45] proposed an authentication model based on ECG Gaussian features with OC'-SVM and incorporate a technique called majority vote to enhance its reliability. To be able to detect post login attacks and support continuous authentication, an extension for FIDO2 and WebAuthn called FIDOnuous was proposed by [43]. Using RFID, RF-Ubia was designed by [31] for authentication that extract user information and biometric characteristic in improving anomaly detection and feature extraction.

Several studies in this domain contribute in terms of usability and acceptance assessment of passwordless authentication in real world and laboratory deployments. A mock setup that deploys FIDO2 hardware token through mobile devices [20], roaming authenticators [32] and FIDO2 roaming software token [21] for authentication was done to conduct and evaluate its usability. To prove the capability of FIDO2 security key as a single factor authenticator, [46] implemented a testbed in large-scale lab study assessing user perception and acceptance and [55] conducted real world deployment to assess its usability. Similarly, a prototype called ExampleTech was designed by [47] that uses WebAuthn protocols to identify users' misconceptions regarding passwordless authentication. On the other hand, [29] executed an extensive laboratory study to assess both the usability and security aspects of Push-Compare-and-Confirm to enhance the security of conventional Push-2FA passwordless mechanism. Security analysis as an objective of study by [23] where a testbed using Windows Hello for Business (WHFB) that uses passwordless as a multifactor was deployed to perform robust evaluation and analysis of WHFB authentication operations.

B. INTERNET OF THINGS (IoT)

Several previewed studies concentrate on Internet of Things, such as studies by [65] offers a secure one'-to'-many authentications and key agreement scheme that utilizes smart card, password, and biometrics for user authenticates to access multiple smart devices simultaneously. Reference [62] put forth CAIAUTH, an authentication framework that uses profiling context on users' behaviours through smartphones and their surroundings through data from gathered from accelerometer and light sensors that can tell apart authorized users from unauthorized ones. Both [63] and [64] uses heart rate, gait, and breathing sounds for authentications in order to provide easier and continuous authentication through those devices. Focusing on Internet of Vehicles, [68] introduces biometric identification for IoV DApp authentication via a scheme called Privacy-preserving and Efficient Biometric Identification (PEBIID) and [69] introduces a resources usage friendly authentication using Mac-based called NoMAS that connects to the internet, with safer communication and security keys updates done with less information sharing. For smart cities, [66] developed fingerprint authentication-based traffic offence control system addressing the constraints of existing systems with real-time data management and [67] proposed user habits for passwordless and continuous authentication using a meta-model-driven approach called WoX+. The latter evaluates the model effectiveness using quantitative and qualitative approaches.

C. PUBLIC SECTOR AND SERVICES

This domain includes services provided in terms of government applications, healthcare, and electronic Identification (eID). Dealing with client-side ballot manipulation, a novel framework leveraging FIDO2 specifications to secure internet voting systems was the product in study by [70]. This authentication framework utilizes WebAuthn with security key and integrated into the online voting system called D-DEMOS. Reference [78] proposed a passwordless scheme to replace password using FIDO called S-Auth for accessing smart energy management application. In healthcare, [76] designed a lightweight multifactor authentication scheme that combines QR code and virtual smartcards. The solution also comes with a secure key management feature that is generated to enable virtual smartcard authentication. Reference [77] presents a new three-factor single sign on (SSO) authentication protocol using smart cards, passwords, and biometrics called Centreless User-Controlled Single Sign-On (CL-UCSSO) for 6G-aided intelligent healthcare systems. Reference [71] unveil a strategy using blockchain as a middle-layer to authenticate users and provide secure access to multiple e-government services without the requirements of another trusted party. This enables a SSO service for users which the authentication done using private and public key pair. In electronic ID realm, [73] introduces enrolment approach for authentication according to requirements of the service provider to balance and compromise between

usability and security by registering national eID as mobile authenticators. This concept was implemented into Electronic Health Records (EHR) Identity and Access Management using an Android application. Reference [57] designed a web application that using Nextcloud combining OpenID Connect protocols with FIDO UAF for a secure smartcard authentication as a second factor for robust identity management and authentication through an application created on android operating system. Reference [75] explores eID's cards as a second factor passwordless authentication using a prototype named FIDELIO implemented a large-scale laboratory study to assess its usability among users. Beside the above eID research, [72] put forth a decentralized digital identity system using FIDO protocols and Verifiable Credentials for the purpose of giving users control over their identities, enhancing trust and preventing user tracking while improving security and privacy through smaller Authentication Authorities. In reducing data leakage in e-government services, [74] promotes the integration of FIDO, SSO and eID as a solution for user identify verification.

D. NETWORK AND INFRASTRUCTURE

Reference [79] Introduces FIDO2CAP prototype via captive portal for user's authentication into a network using FIDO2 security key authenticators. Reference [80] proposed a middleware to allow authentication using FIDO protocol of asymmetric key pair to authenticate to cloud SAAS service without the need to recode the SAAS applications. The credentials keys are stored in a database inside the SAAS application, and the key management utilizes the Amazon Web Service Key Management. Reference [81] Introduces SIMBA for user authentication to commodity Services using SIM cards inside phones. Specifically used in telecommunication for mobile users' identity verification, it enables passwordless authentication to be done with minimal MNO dependency and uses sub-profiles for multiple secure logins to services. Reference [82] introduces passwordless authentication 1FA solution for OpenStack private cloud. The solution uses REST API and JSON to connect to a FIDO2 Identity server or relying party for authentication through the modified login page that invoke the API calls. Reference [83] develops an intermediary web portal for secure VPN access using FIDO2 keys. The web portal will invoke restful API to communicate to a radius server for identification purposes. Reference [84] proposes environment-independent user authentication using channel state information (CSI) in WiFi signal that detects behavioural patterns. This solution includes 2 deep-learning models of convolutional neural networks (CNN) that analyse behaviour via time and frequency of actions. Reference [85] developed an innovative multi-factor, multi-layer authentication framework that has passwordless as another layer of authentication to enhance cloud security. This solution features access control and intrusion detection mechanisms, that automatically select the most suitable authentication methods for users.

E. BUSINESS AND ECONOMY

Reference [89] Developed a prototype called Genuine mobile money (G-MoMo) that uses multi-factor authentication algorithm for mobile money applications that combines PIN, OTP, biometric fingerprint, and QR code for authentication to Ensure data confidentiality, integrity, non-repudiation, user anonymity, and privacy. It utilized SHA-256 to encrypt the OTP, RSA encryption, and Fernet encryption for QR Code. Reference [88] uses FIDO protocols for biometric authentication control integrated into a ticketing sale system for the purpose of seat management and ticket scalping prevention during sports events. Reference [91] introduces a user-centric identity system for online banking through a novel Universal Authentication and Authorization Framework (UAAF) that uses FIDO UAF protocols for authentication. This solution is also integrated with multiple issuers for digital identity verification that provides reliable attributes to ensure the identity of users in online banking transactions. Reference [86] proposed digital custody model integrates FIDO and DID authentications with enhanced security features. This model incorporates an implemented biometric sensor featuring an encryption module to bolster security measures. It uses a home gateway to enable secure storage and access to digital assets and a hardware DID-based biometric authentication to identify and verify user in this framework. Reference [90] pioneers a cardless cash withdrawal in ATM machines that uses Infra-Red (IR) radiation to authenticate and verify users through their palm veins. Reference [87] applied FIDO2 specifications into padlocks that provides passwordless mechanisms to these locks in securing physical assets. The physical authenticator data is stored in the cloud for security purposes and is only accessed when an unlock is requested by the user. The solution also provides a cloud web-based physical key management for adding or removing keys.

F. EDUCATION AND RESEARCH

Leveraging the use digital certificates issued by a certification authority as a second factor of authentication, a plugin developed by [94] to access the Moodle E-Learning platform. To prevent fraud in online examination, [92] proposed a framework consisting of edge computing and machine learning model to enable static and continuous authentication using keystroke dynamics equipped with Gaussian model-based anomaly detector and keystroke stream processor. Reference [95] introduces a new, open-source solution for multi-factor authentication (MFA) specifically designed for Shibboleth Identity Providers that aims to significantly to enhance access to university application by adding three additional second factors: One-Time Password, FIDO2, and Phone Prompt. Reference [93] creates an intermediary Identity Management (IDM) that allows the use of token-based authentication as an additional factor for Technical Coordination Services (TCS) in the EPOS research system This enable users to manage their credentials more efficiently, thus

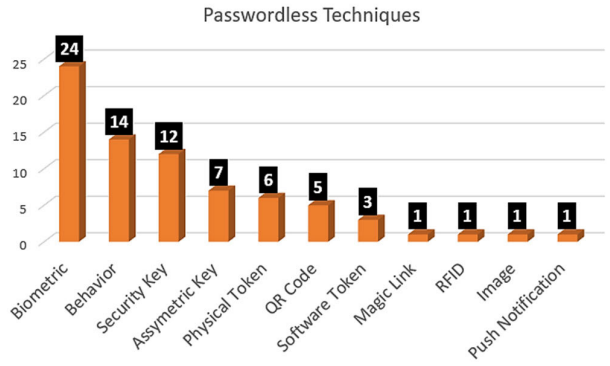


FIGURE 8. Distribution of passwordless methods and techniques used in previewed studies.

simplifying the process of accessing various research services offered in the EPOS project.

G. LIFESTYLE AND TOURISM

Reference [98] developed a lightweight privacy preserving authentication by using software and FIDO token in a smart hotel context for reservation and authorizing user access to the hotel room after checking in. This mechanism uses NFC, Zigbee and WiFi to communicate the user's phone with the servers. In the realm of visual space, [97] applied FIDO2 standards in a solution called Metasecure where users can authenticate and manage their identity via facial recognition and a security key or smartcards (authentication via phone). This study also provides SDKs for any system including VR/XR glasses. Similarly, [96] presents two solutions. First, is Kalεido, a practical privacy mechanism that maintains the functionality of eye-tracking systems while safeguarding user privacy in real-time. Second, the author presents Velody a method of biometric authentication based on challenge-response with the objective to mitigate the security vulnerabilities linked to breaches of biometric templates. This study also explores the impact of user interaction experiences on the security perceptions of authentication methods in virtual reality environments.

H. AGRICULTURE

Gesture Tapping Rhythm, which is a method that captures a unique set of user rhythm created by tapping onto the screen for agricultural workers to authenticate while they work was suggested by [99]. It leverages accelerometers and gyroscope features in a mobile phone integrated with a machine leaning model based using SVM-rbf.

VII. DEPLOYED PASSWORDLESS TECHNIQUE

There are various methods without passwords that have been explored and deployed by researchers in the selected papers to solve the problems that has been identified. TABLE 7 and FIGURE 8 below shows a list of passwordless methods that have been applied either as the first factor or as an additional factor to password authentication.

TABLE 7. Passwordless techniques used in selected papers.

Passwordless techniques	Papers
Biometrics	[19], [23], [28], [37], [41], [47], [50], [54], [58], [59], [66], [68], [69], [72], [73], [77], [78], [82], [86], [88], [89], [90], [91], [96]
Behavioural	[24], [32], [33], [34], [35], [44], [45], [62], [63], [64], [67], [84], [92], [99]
Security keys	[20], [22], [36], [46], [48], [55], [70], [79], [83], [87], [95], [97]
Asymmetric keys	[26], [27], [36], [39], [53], [71], [94]
Physical Tokens	[42], [57], [74], [75], [81], [100]
QR Code	[19], [40] [49] [74] [76].
Software Token	[21], [93], [98]
Image	[38], [51]
Push Notification	[29]
Magic Link	[30].
RFID	[31]

A. BIOMETRICS

Most of the previewed studies delved into biometrics as the preferred passwordless authentication either as the first factor or second factor. The most biometrics of choice are fingerprints. FIDO protocols for fingerprints authentication were implemented in [28], [78], and [91] while [66], [69], and [86] doesn't following any FIDO standards. Fingerprints are also integrated with other products such as OpenStack [82] and open-source EC-CUBE system [88]. Besides that, [68] introduce a fingerprint identification scheme that uses invertible matrix. Besides fingerprint, face detection is also used in studies [19], [23], [47], iris recognition [37], [41] and the use of palm vein [90]. This is most probably due to due to their convenience, accuracy, and enhanced security features that offers reliable and unique identification methods for various applications ranging from personal devices to access control systems. The inherent availability of biometrics in the market is also a contributing factor, pushing towards passwordless technology as most smartphones are equipped with fingerprint sensors and face recognition features.

B. BEHAVIORAL AUTHENTICATION

Behavioural authentication techniques refer to identity authentication using individual behaviour patterns such as typing patterns, online browsing patterns, or device usage patterns. Most of these authentication methods use machine learning to support and process authentication methods.

One of the behaviour verification techniques is based on keystroke dynamics [32], [35], [92], heartbeat, gait, and audio breathing [63], [64], handwriting [34], WiFi signals [84], human rhythm through phone tapping [99] and activity patterns when interacting with their phones [44]. BehaviorID, a passwordless authentication that proposed by [24] uses a different behaviour mechanism that is based on certain triggers such as actions in banking apps, email, and social services. BioDraw, a solution by [33] combines several factors including impedance, geometry, composition, and behaviour with passwords pattern swiped on a RFID tag array for user identification and authentication. Interestingly, this concept is gaining increased attention due to the increasing number of smart devices as it offers an additional way to verify a user's identity that is easy and effortless.

C. SECURITY KEYS

Security keys such as Yubikey, Google Titan Security Key and RSA SecurID have been marketed and are easily available online. It can be used through USB and NFC. Studies that have been carried out using security keys as the first factor [20], [46], [55] while [22] and [70] use it as an additional factor. Although to be very secure compared to password, it suffers due to usability issues.

D. ASSYMETRIC KEYS

One of the methods to achieve passwordless authentication is to use asymmetric keys such as passkeys, digital certificates, and public key infrastructure (PKI). PKI is a system designed to manage digital certificates by combining public keys with digital signatures to ensure authentication and maintain data confidentiality. PKI and passkeys leverage asymmetric cryptography, where each key pair creation involves a public key for wide distribution and a private key for secure storage. PKI was used by [27] and [39] in their proposed solutions. Reference [94] introduces digital certificates as a second factor while [53] uses the passkey method introduce by FIDO.

E. PHYSICAL TOKENS

Other than security key, there is another form of physical token that integrates a chip, or an integrated circuit card (ICC) is a small thin factor such as smart card, ID Card, and passports. Smart cards serve as secure portable storage devices that can be used across various applications to facilitate access to an online or offline systems environment. Reference [65] presented a smart card-based authentication scheme alongside password and biometrics adapted for IIoT whereas [57] for web applications. Studies by [74] and [75] integrate eID as passwordless authentication using an ID Card as the second factor. Reference [42] also introduced an authentication framework called FIDO-AC by integrating eID but using ePassport physical tokens. Another type of physical token in the form of SIM cards are also used to authenticate users into telecommunication networks [81].

F. QR CODE

The QR code method is also used as a passwordless method technique. Reference [40] introduced QR for improvements to the registration and authentication procedure of FIDO2 external authenticators while [49] uses QR code as FIDO2 protocol alternative. Reference [74] integrates FIDO and eID for SSO using QR code as authentication. QR codes are used as a second factor along with smart cards for authentication [76].

G. SOFTWARE TOKENS

Another type of passwordless authentication methods that were implemented in the selected studies are software-based tokens. Studies in [93] allows to authenticate in different research services and resources using a generated software JWT token after a user has initially logged into the system using one of the several identity providers services. For smart hotel services, [98] implemented a lightweight public key token that are stored in a user smartphone after initial login setup and reservation. This token then can be used by users during accommodation especially in interacting with IoT devices such as smart lock to access their room and other devices in those rooms. In addition, study in [21] explore the usage of software token in smartphone as a mobile authenticator in replacing physical security keys.

H. OTHER PASSWORDLESS TECHNIQUES

Apart from the commonly used techniques as mentioned above, several other methods are use in implementing passwordless authentication such as magic links, push notification, RFID and image-based authentication. Magic link authentication usually uses email as medium where the link for authentication is set. Only one study in the selected paper implements this technique [30]. The lack of study on this mechanism may be due to the availability of other passwordless that are more robust and secure.

Push notification is another passwordless mechanism that is applicable as a first or second factor. One study [29] proposed an improvement of push notification technique is called Op-2FA for improvement of security issues in traditional push notification technique. Although this technique gained widespread a few years back, especially in the banking sector, the decline of new innovative solutions using push notification is apparent.

Besides the above, study by [31] uses RFID with finger movement detection for physical access and solution in [51] uses an authentication technique using a camera and photo captured to detect the correct URL on the browser title bar while [38] uses images to verify and authorize a user.

VIII. METRICS USED IN EVALUATING PASSWORDLESS AUTHENTICATION SOLUTIONS

Performance evaluation is a crucial step for assessing the effectiveness and efficiency of the solutions proposed in the reviewed papers. This research question aims to identify and

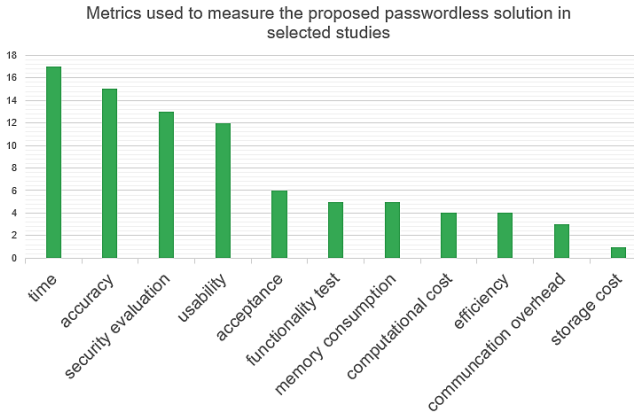


FIGURE 9. Distribution of metrics used in selected studies.

TABLE 8. Evaluation metrics used in selected studies.

Metrics	Papers
Time	[25], [31], [36], [39], [40], [42], [43], [47], [52], [57], [65], [68], [69], [71], [75], [87], [97]
Accuracy	[19], [24], [31], [33], [35], [37], [45], [51], [63], [64], [84], [85], [93], [96], [99]
Security Evaluation	[40], [53], [56], [69], [77], [81] [23], [48], [60], [65], [76], [81] [89]
Usability	[20], [43], [46], [48], [54], [55], [59], [75], [88], [95] [48], [59].
Acceptance	[21], [22], [45], [55], [66], [79].
Functionality Test	[50], [65], [77], [81], [95]
Computational Cost	[39], [65], [69], [89]
Efficiency	[39], [48], [76], [94]
Memory	[38], [39], [65], [77], [89]
Communication overhead	[48], [69], [89]
Storage	[77]

analyse the specific metrics employed to measure the performance of authentication solutions. This is to understand the criteria used to evaluate performance and give insights to the common metric used in evaluating performance of passwordless solutions. Based on the reviewed paper, approximately 83 % of these studies conducted performance evaluation. The metrics that have been used are as shown in FIGURE 9 and TABLE 8. Topmost used metrics are time, followed by accuracy, security performance, usability, and acceptance.

A. TIME

Time factor is the most used metric in the selected reviewed papers. Time assessment includes the measurement of time to authenticate [36], [40], [65] time to register [40], [71], [87], token exchange time [25], token validation time [57], time performance [42], processing overhead [43], setup time [75], and execution times [39], [69]. The importance of this metric in authentication is due to requirements of a fast mechanism to access or gain a particular service as slow authentication process will hinder its usability. The time measurement recorded for these above-mentioned papers are as TABLE 9.

TABLE 9. Sample of time measurement used and its result.

Papers	Purpose of Time Measurement	Results
[65]	authenticate	0.396 ms for overall cryptographic runtime
[36]	authenticate	150ms using FIDO2
[40]	register and authenticate	141ms for authentication 373ms for registration
[71]	register	0.8s
[87]	register	5.794ms registration 4.964ms authentication
[25]	token exchange	Inside Office environment takes 1151ms while remote users take maximum 1586 ms
[57]	token validation	averaged 150 ms
[42]	time performance	Average 5.18s
[43]	Processing overhead during registration	1.3 seconds with 19 fragments at 20 bytes and 50 milliseconds with 1 fragment at 512 bytes
[75]	Setup for second factor	5 minutes and 37.5seconds
[39]	Execution of RSA function	Without TEE: 0.321741 seconds With TEE: 1.102976 seconds
[69]	Execution of all cryptographic function	Using Desktop: 133.2 ms Using Raspberry Pi: 201.41 ms

B. ACCURACY

Accuracy is the second most used metric after time. It encompasses of AUC-ROC and RMSE [63], [64], False Acceptance Rate (FAR) [24], [37], Equal Error Rate (EER) [35], False Negative Rate (FNR) [96], False Positive Rate (FPR) [31], [84], F-Score [45], True Acceptance Rate (TAR) [99], Precision [51] to gauge the accuracy of the passwordless solutions that has been proposed. This metrics are used in AI or machine learning mechanism that integrated in the passwordless solutions. Accuracy is another important factor as it ensures authentication reliability. TABLE 10 shows each type of accuracy measurement used for it specific purposes and sample result based on the above findings.

C. SECURITY EVALUATION

Security analysis is the third preferred metric used to evaluate the solutions. Studies in [40], [53], [56], [69], [77], and [81] used formal verification techniques to evaluate the security protocols and flows. In paper [23], [48], [60], [65], [76], [81] followed an informal approach where the analysis was done through deductive and heuristic approaches that involved educated guess or common-sense principles. Paper [89] conducts a security comparison analysis to password-based authentication.

TABLE 10. Sample of accuracy measurement used and its results.

Paper	Purpose of accuracy measurement	Result
[63]	To evaluate model's ability to distinguish between two classes using AUC-ROC and differences between predicted values and observed values using RMSE.	average AUC-ROC 0.91 ± 0.02 which show excellent performance. The RMSE results show that k-NN and SVM (RBF kernel) provide the most well-calibrated probability predictions with the lowest RMSE of 0.27
[64]	To evaluate model's ability to distinguish between two classes using AUC-ROC	The HIAuth model using SVM classifier with RBF kernel achieve AUC-ROC of 0.94 ± 0.03 during sedentary period and AUC-ROC of 0.98 ± 0.04 during non-sedentary period
[24]	measures the rate at which unauthorized individuals are incorrectly accepted using FAR	FAR result is 0.3%
[37]	measures the rate at which unauthorized individuals are incorrectly accepted using FAR	FAR results shows excellent security at thresholds (0.06% at 1%), but a sharp increase to 5.67% at over restrictive thresholds (0.01%)
[35]	To compare different models from multiple deep learning model with addition of keystroke dynamics using EER	Achieve the best EER = 4.89% using GoogleNet Deep Learning Model
[96]	Evaluate Velody authentication usability and reliability by determining how often legitimate users are incorrectly rejected using FNR.	FNR of 10.7% in intra-day sessions and 11.8% in inter-day sessions that achieve balance between usability and security
[31]	measures RF-Bia's ability to block illegitimate users using FPR	FPR doesn't exceed 0.04
[84]	evaluate the system's robustness against unauthorized access by measuring the proportion of unauthorized users' behaviours incorrectly classified as legitimate using FPR	FPR is below 1% for random attack and below 2% for mimic attack
[45]	measure how well the authentication system balances recognizing legitimate users correctly and rejecting imposters using F-Score	F-score of 98.44%
[99]	evaluate the system's ability to correctly recognize valid users during authentication using TAR	TAR result 96.54%
[51]	evaluate the accuracy of the system in correctly identifying and authenticating objects or actions without falsely identifying others using precision	Domain name OCR: 95.87% Address bar detection: 98.22% precision for known browsers and 93.81% precision for unknown browsers.

D. USABILITY

Usability is one of the performance metrics that is used to evaluate the authentication methods that has been proposed. This study is usually done using qualitative and quantitative such as in studies [54], [59], [75] where applying the solutions into real world environments or labs experiments equipped with survey and/or interviews. This metric also gauges the deployability of the solutions [48], [59].

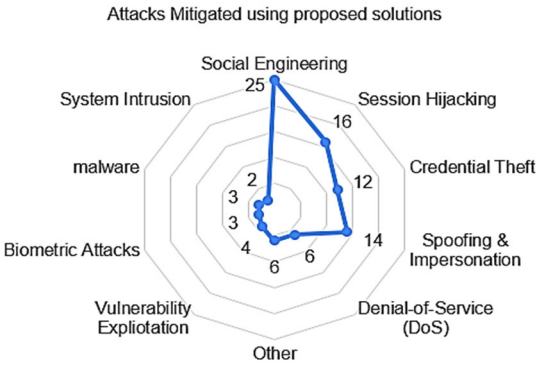


FIGURE 10. Distribution of types of attack that can be mitigated ased on previewed studies.

E. ACCEPTANCE

Acceptance evaluation is a measurement that focus on users' overall willingness to use the proposed authentication solutions. This includes user acceptance,ratings, reviews, perception [22], [66], [79]. Both usability and acceptance evaluation are conducted using surveys and lab experiments that require users' feedback.

F. OTHER METRICS

Some other notable metrics used are such as storage cost, memory consumption, functionality, computational cost, and efficiency. Papers in [39], [48], [76], and [94] gauge the efficiency of the passwordless mechanism. The storage cost was measured in [77] to identify the size of the storage needed. Besides storage, memory consumption [65], [77], [89] and overall computational cost are [39], [69] used to evaluate the proposed scheme identify whether there is any potential bottleneck in terms of resources requirement that can degrade the performance. Functionality of the solutions that was proposed in [50], [65], and [81] were tested to conform to the intended design and requirements stated in each study objectives. Lastly, communication overheads are measured in [48], [69], and [89].

IX. ATTACK MITIGATED BY USING PASSWORDLESS TECHNIQUE

In the reviewed papers, the authentication methods that incorporate passwordless mechanisms were designed to enhance the security fortitude and robustness. Summary of the security attacks that can be mitigated as shown in FIGURE 10 and TABLE 11.

A. SOCIAL ENGINEERING

The most common attacks associated in the reviewed papers that can be prevented are Social Engineering [53], [89]. Social engineering involves manipulating individuals to divulge confidential information or perform actions that compromise security protocols. This attack also includes Phishing

TABLE 11. Types of attacks mitigated in selected studies.

Types of Attack Mitigated	Papers
Social Engineering	[22], [23], [26], [31], [36], [47], [49], [51], [52], [53], [54], [55], [56], [59], [62], [72], [73], [75], [76], [79], [82], [83], [87], [89], [95].
Session Hijacking	[23], [26], [33], [40], [49], [59], [60], [61], [65], [69], [76], [81], [83], [85], [87], [89]
Spoofing And Impersonation	[24], [39], [44], [51], [60], [65], [76], [77], [84], [89], [95], [96], [98], [99]
Credential Theft	[19], [23], [30], [34], [44], [48], [50], [72], [76], [78], [79], [89]
Denial of Service	[36], [61], [65], [71], [77], [85]
Biometric Attacks	[37], [86], [97]
Vulnerability Exploitation	[23], [33], [39], [81]
Malware Based Attacks	[22], [56], [85]
System Intrusion	[82], [86]
Others	[31], [33], [71], [74], [76], [84]

attack [22], [36], [72], Shoulder surfing [89], and Mimicry attack [31], [62]. Utilizing passwordless mechanisms helps mitigate these threats by adding an extra layer of security through alternative authentication methods such as biometrics or token-based authentication, significantly reducing the susceptibility to these types of attacks.

B. SESSION HIJACKING

Session hijacking involves unauthorized interception or takeover of an ongoing session between a user and a system that can allow attackers to assume control of the session and potentially access sensitive data. Session hijacking which includes attacks such as Replay attack [40], [49], [83], Session-specific temporary information attack [65] and Man-in-the-middle attack [49], [59], [85] presented as attacks that can be prevented.

C. SPOOFING AND IMPERSONATION

Spoofing and impersonation are techniques that use falsified data or identities to deceive systems or individuals in order to gain access masked as a legitimate user. This type of attack which includes spoofing attack [24], [44], [99], user or device impersonation attack and Token impersonation [98], Stolen verifier attack [76], homographic phishing attacks and Domain injection attacks [51] were able to be mitigated when implementing passwordless mechanisms.

D. CREDENTIAL THEFT

Credential theft-based attack are attacks that used to gain a person identity for authentication and authorization. This attack includes Brute force attack [34], [76], [78], Credential stuffing [50], PIN Guessing [89], Dictionary attack and key-loggers [23]. Using passwordless as the first factor eliminates passwordless entirely while as an additional factor provides additional strength even if password has been leaked or stolen.

E. DENIAL OF SERVICE (DOS)

DOS attack is an attack where a malicious actor tries to make a computer resource unavailable to its intended users by disrupting services, often by overwhelming the target system with excessive requests. Passwordless solutions proposed in [36], [61], [65], [71], [77], and [85] can help mitigate this type of attack.

F. BIOMETRIC ATTACKS

Biometrics attack involve attempts to compromise biometric authentication systems to gain unauthorized access. These attacks were able to be prevented in solutions proposed in [37], [86], and [97].

G. VULNERABILITY EXPLOITATION

Exploitation of weakness and vulnerabilities is to take advantage of weaknesses or vulnerabilities in a particular system to gain unauthorized access. Based on the reviewed studies in [23], [33], [39], and [81], these attacks can be prevented by the passwordless solutions that has been proposed.

H. MALWARE-BASED ATTACK

This type of attack uses malicious software called malware to compromise or gain unauthorize access to a system. Passwordless solutions provided in studies [22], [56], [85] can eliminate this attack from gaining access and causing damages.

I. SYSTEM INTRUSION

System Intrusion refers to unauthorized access into a computer system or network that often with malicious intent such as stealing user or corporate data. Passwordless mechanism that are proposed in [82] and [86] helps preventing this kind of attack.

J. OTHER TYPES OF ATTACK

Several other exploits that can also be prevented are such as pattern behavioural attack [33], QRLJacking [74], data manipulation [71], modification attack [76], and random attack [31], [84]. Based on these findings from the reviewed papers, TABLE 12 shows the passwordless mechanism used in these papers that correspond to which attack that the mechanism able to mitigate and prevented.

X. ISSUES, CHALLENGES AND LIMITATIONS

Based on previous studies on passwordless authentication, this paper analyses all the selected studies to extract information regarding limitations, issues and weaknesses that

TABLE 12. The mitigation of attacks corresponds to the type of passwordless mechanism implemented.

Attack Category	Attack Method	Paper	Passwordless Mechanism Used
Social Engineering	Phishing Attack	[22] [36]	Security Key
		[72]	Biometric
	Shoulder Surfing	[89]	Biometric
	Mimicry Attack	[31]	RFID
		[62]	Behaviour
Session Hijacking	Replay Attack	[40] [49]	QR Code
		[83]	Security Key
	Session-specific Temporary Info Attack	[65]	Physical Token (ID Card)
	Man-in-the-middle Attack	[49]	QR Code
		[59]	Biometric
		[85]	Security token sent via email and fingerprint
Spoofing and Impersonation	Spoofing Attack	[24] [44] [99]	Behaviour
	Token Impersonation	[98]	Software token
	Stolen Verifier Attack	[76]	Virtual Smart Card and QR Code
	Homographic Phishing, Domain Injection	[51]	Photo Based Authentication
Credential Theft	Brute Force Attack	[34]	Behaviour
		[76]	Virtual Smart Card and QR Code
		[78]	Biometric
	Credential Stuffing	[50]	Biometric
	PIN Guessing	[89]	Biometric
	Dictionary Attack, Keyloggers	[23]	Biometric
Denial of Service (DoS)	Overloading Service Requests	[36]	Security Key
		[61]	Attribute Based Authentication leveraging Blockchain
		[65]	Physical Token (ID Card)
		[71]	PKI integrated with Blockchain
		[77]	Biometric
		[85]	Security token sent via email and fingerprint
Biometric Attack	Biometric System Compromise	[37], [86]	Biometric
		[97]	Biometric and Security Key
Vulnerability Exploitation	Exploitation of System Weakness	[23]	Biometric
		[33]	Behaviour
		[39]	PKI
		[81]	Physical Token (SIM Card)
Malware-Based Attack	Unauthorized Access via Malware	[22]	Security Key
		[56]	Asymmetric Key

TABLE 12. *(Continued.)* **The mitigation of attacks corresponds to the type of passwordless mechanism implemented.**

System Intrusion	Unauthorized System Access	[82] [86]	Biometric
Other Types of Attack	Pattern Behavioural Attack	[33]	Behaviour
	QRLJacking	[74]	QR Code and Physical Token (ID Card)
	Data Manipulation	[71]	PKI integrated with Blockchain
	Modification Attack	[76]	Virtual Smart Card and QR Code
	Random Attack	[31]	RFID
		[84]	Behaviour

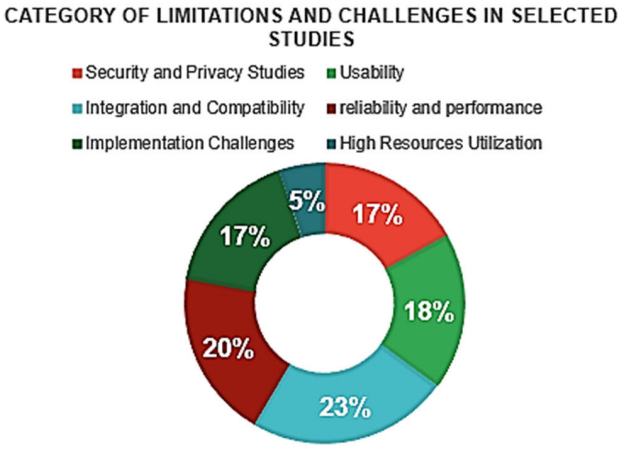


FIGURE 11. **Limitations and challenges in the selected studies.**

TABLE 13. **Limitation and challenges in selected studies.**

Limitation and Challenges	Papers
Integration And Compatibility	[25], [27], [28], [42], [52], [53], [56], [61], [62], [66], [73], [74], [79], [80], [82], [83], [93], [98]
Performance And Reliability	[24], [32], [33], [34], [35], [41], [44], [45], [51], [58], [63], [64], [67], [84], [99]
Usability	[20], [21], [22], [46], [47], [49], [54], [55], [60], [75], [77], [85], [88], [95]
Security And Privacy	[29], [30], [31], [36], [37], [50], [59], [70], [76], [78], [90], [94], [96]
Implementation Challenges	[19], [23], [43], [48], [57], [65], [68], [69], [72], [86], [87], [89], [91]
High Resources Utilization	[39], [40], [71], [92]

have been identified and encountered on the solutions that has been proposed. These issues and weaknesses have been grouped into several categories as provided in FIGURE 11 and TABLE 13.

A. INTEGRATION AND COMPATIBILITY

Some of the passwordless authentication solutions proposed are developed using or focusing on specific browsers [56], [79], platforms such as AWS cloud [80] or OpenStack [82],

Trusted platform module (TPM) 2.0 [62], network environment [25], operating systems such as android [27], [66], [73] or to a very specific use case [61] which may cause these solutions to be incompatible or unable to be adopted in different settings. In the study by [83] states that there are legacy VPN systems that do not support authentication based on websites and VPN clients may not be able to perform authentication using the FIDO2 protocol. Effective authentication needs to consider the requirements of different platforms and operating systems to ensure that it can be widely used by a variety of users.

B. PERFORMANCE AND RELIABILITY

The performance of passwordless authentication solutions that is less accurate can be seen in studies [24], [41], [58]. Limited samples on studies [63], [67], [99] while giving a good result, may lead to performance accuracy and reliability issue when applied to a broader population. This limitation can result in skewed data that does not fully represent the diversity of the larger group. Slow performances are also highlighted in studies [35], [45]. Adverse effects caused by jewellery or wearables can cause accuracy issues [33].

C. USABILITY

The proposed authentication technique receives criticism from users when there is a need to use an additional device that needs to be carried all the time for authentication purposes [22]. The lack of account recovery techniques in the FIDO standard due to the loss or theft of devices such as physical security keys or smartphones that can render the account inaccessible which also impacts the usability of passwordless authentication [20], [49], [60], [75]. In addition, the need for repeated registration for various online applications was also identified as an obstacle to the

smoothness of authentication for the proposed FIDO protocol using passkeys and security keys. Due to the design of the authentication protocol, [47], [54], [55] mentioned

that registration and authentication on each application even within the same domain of services requires separated registration and repetitive authentication process due to the unique key pair generated for each of the services. The complicated design of the system is perceived as a usability issue [88]. Additionally, error caused by security keys and error handling by different servers has also been cited as degrading usability [95]. Reliance of multifactor authentication has been highlighted as a burden for users [77], [85]. The usability of authentication that reduces user burden needs to be considered to ensure that users can use authentication that is not only safe but also easier and more practical.

D. SECURITY AND PRIVACY

Concerns regarding security and privacy above the study can be seen in the studies that have been carried out. Most of the security issues that can still be seen are because there are uses that still depend on the use of passwords [31], [36], [78], PIN and OTP [90] and the need for a password manager [50] even though there are obvious weaknesses and usage issues. The authentication method through push notification authentication is vulnerable to vulnerabilities such as HEINA attacks [29]. Proposed authentication techniques that use email [30], [70] are likely to be vulnerable to other cyber-attacks. Relying on email delivery also has obvious limitations such as being marked as spam, bounced by servers, and intercepted by third party. References [37] and [96] stated in the study that the verification techniques presented are likely to face new sophisticated attacks in the future. The need for more secure authentication techniques considering weaknesses and vulnerabilities is an important aspect to provide trust to users.

E. IMPLEMENTATION CHALLENGES

The implementation of authentication methods has been studied and highlighted as likely to have challenges when implemented in the real world. First, additional components are required and may lead to additional implementation costs that may hinder the implementation of the proposed solution [68], [86], [87]. Other requirements, initial setup and regulation may also factor in as challenges in deployment [72], [91]. The need to migrate existing accounts to [23] and [48] is deemed as a burden. Other than that, solutions by [19] requires high storage cost due to the number of photos needed to be stored for the authentication. [89] proposed solution is having a complexity for deployment as its required 4 different applications to be installed. Therefore, the implementation of passwordless needs to address these implementation challenges for easier deployment and non-costly implementations.

F. HIGH RESOURCES UTILIZATION

The study carried out by [39], [40], [71], and [92] is seen to require a high use of resources in terms of CPU processing capabilities. Thus, there is an importance for authentication techniques without passwords that are light, efficient and do not require high processing capabilities.

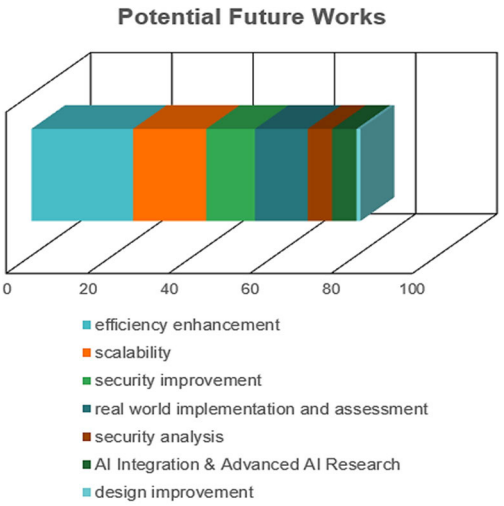


FIGURE 12. Distribution of category of potential future works.

XI. FUTURE OPPORTUNITIES AND IMPROVEMENTS

There is an importance in outlining future directions within the realm of passwordless authentication towards user identification. These directions can serve as guiding principles for researchers to propel the field forward, address novel challenges, and broaden the application of authentication protocols. They serve as focal points for researchers to enhance security, efficiency, and practical implementation while exploring new innovative ideas and embracing new technologies. In this paper, future research opportunities are organized into common themes to create a thorough roadmap that researchers can identify in promoting new innovations and progression in passwordless authentication studies as shown in FIGURE 12 and TABLE 14.

A. EFFICIENCY ENHANCEMENT

Studies in [36], [54], and [71] highlighted the enhancement of the features of passwordless authentication for a better efficiency and effective solution as a possible area for future improvements. This is to streamline the authentication process, reduce friction for users, increase usability, acceptance and optimize resource utilization.

B. REAL WORLD IMPLEMENTATION AND ASSESSMENT

While theoretical proposals for novel authentication methods are valuable, the true test lies in their real-world application. Practical implementation is deemed crucial and important in studies [76], [79], [94] as the assessment can verify the authentication solutions in terms of effectiveness, scalability, and resiliencies. It also provides a better understanding of user perceptions and acceptance, and the usability of the solutions to enhance its capabilities for widespread adoption.

TABLE 14. Category of potential future works.

Potential Future Works	Papers
Efficiency Enhancement	[21], [22], [24], [25], [26], [31], [32], [35], [36], [39], [41], [44], [46], [54], [62], [69], [71], [73], [75], [82], [84], [88], [90]
Real World Implementation and Assessment	[20], [43], [45], [48], [52], [61], [63], [64], [76], [79], [87], [89], [94]
Scalability	[28], [42], [50], [51], [53], [56], [57], [59], [66], [72], [74], [78], [81], [83], [91], [92], [95], [99],
Security Improvement	[19], [27], [29], [30], [55], [58], [65], [77], [85], [93], [96], [97]
Security Analysis	[23], [38], [40], [49], [60], [70]
AI And Machine Learning Integration	[34], [37], [67], [68], [80], [98],
Design Improvement	[47]

C. SCALABILITY

As shown in papers [56], [57], [83], [99], improvement in the solutions scalability is one of the pointed future works that can be explored. This is due to the importance of a passwordless solution that can seamlessly scale up to an IT setup that usually grows within time, and using multiples environment such as different operating systems, architecture, and deployment of IT infrastructure.

D. SECURITY IMPROVEMENT

Improving security is evident in studies [65], [85], [97] the field continues to evolve, constantly seeking improved solutions to address new and different types of cyber threats. This ongoing pursuit aims to fortify the security of proposed solutions and ensure robust protection against evolving risks and challenges.

E. SECURITY ANALYSIS

Papers [23], [49], [60] suggested to conduct further security evaluation on passwordless solutions that have been represented. This future direction aims to deepen the understanding of the strengths and weaknesses of these solutions, thus facilitating refinements of the security measures and protocols used in these solutions. This analysis will contribute to the development of more resilient and trustworthy passwordless authentication methods while enhancing overall security in digital environments.

F. AI AND MACHINE LEARNING INTEGRATION

As pointed out in papers [67], [68], [80], introducing AI and machine learning in the authentication realm is an area that can be explored for further advancement. With the capabilities of AI and machine learning algorithms, there is potential of revolutionizing authentication processes by enhancing accuracy, adaptability, and responsiveness. These technologies can analyse vast amounts of data to identify patterns, anomalies, and potential threats in real-time. Therefore, security measures can be bolstered while facilitating user experience improvement.

G. DESIGN IMPROVEMENT

Paper [47] suggested that future research involves much better design of the authentication interfaces. This direction aims to promote a much better usability and increase user friendliness in promoting the passwordless solutions.

XII. DISCUSSION

Passwordless authentication offers substantial benefits over traditional password-based systems that improved security, enhanced usability, and scalability across diverse domains. However, as highlighted in the reviewed studies, its effectiveness depends on the specific application context and domain requirements. In high-security environments like healthcare, multi-modal biometric systems combining face and fingerprint data [19] or advanced behavioural authentication methods such as [24] and keystroke dynamics [78] provide reliable solutions for preventing unauthorized access. These approaches are well-suited to sectors where user identity verification is critical, and security risks are significant. Furthermore, innovations such as combining iris detection with pupil diameter measurements [37] and leveraging eye movement detection [41] enhance biometric authentication for applications requiring robust security.

In contrast of other domains such as IoT and agriculture, lightweight solutions are prioritized to accommodate resource-constrained environments and scalability needs. For instance, gesture-based tapping rhythm for agricultural workers [99] where devices must balance simplicity with efficiency. Similarly, virtual smartcards [76], decentralized digital identity systems [72] and FIDO2-based frameworks [57], [73] enhance usability and privacy in the public service applications although it may face challenges in adoption due to integration and infrastructure requirements. These examples demonstrate that passwordless authentication deployment must align with the unique needs of each domain to balance security, usability, and scalability effectively.

Different passwordless authentication mechanisms exhibit varying strengths and limitations, making them more suitable for a particular application. Biometric authentication, such as fingerprints and facial recognition is ideal for high-security environments like healthcare and finance to ensure unique user identification is paramount and security risks are significant. Conversely, behavioural authentication that leverages patterns like keystrokes or smartphone interaction is better suited for IoT and smart city applications that require continuous and adaptive authentication to handle dynamic user behaviour and device interactions. Security keys and cryptographic tokens like FIDO2, are highly effective in enterprise and network infrastructure settings, where robust

protection against phishing and man-in-the-middle attacks is crucial. On the other hand, lightweight mechanisms such as gesture-based systems excel in resource-constrained environments such as agriculture due to their simplicity and ease of implementation. These distinctions highlight that the suitability of a passwordless mechanism depends on its ability to balance security, usability, and scalability with the specific requirements of the application domain.

The state of the art in passwordless authentication primarily revolves around the adoption of technologies like biometrics, behavioural patterns, and cryptographic mechanisms such as FIDO2 and WebAuthn protocols. As reviewed in this paper, these solutions have been applied to enhance security in sectors like finance, healthcare, and IoT. However, existing studies often focus narrowly on specific mechanisms or domains, leaving gaps in comparative evaluations, especially in scalability and real-world implementation challenges. In contrast, the findings in this paper provide a broader perspective by systematically comparing multiple passwordless mechanisms across diverse domains such as healthcare, IoT, education, and public services. Unlike prior works, the consolidation of these mechanisms presented by identifying performance metrics, ability to mitigate specific attacks, issues and limitation highlights new insight regarding their applicability across environments with varying resource constraints and purposes. Based on these findings, there are still challenges and constraint on adopting passwordless solutions. However, new novel opportunities have been underline are especially in real-world deployment scenarios can be explored which are often underexplored in existing literature and help lays the groundwork for future advancements in passwordless authentication.

XIII. CONCLUSION

In conclusion, this study provides an in-depth exploration of passwordless authentication across various environments. Authentication is the first line of defence against unauthorized access, ensuring that only authorized users can interact with systems, thereby establishing a secure foundation for subsequent communication [100]. Through a comprehensive literature review, the research evaluates relevant works that employ passwordless authentication as either a primary or supplementary factor, identifying key challenges and issues. Additionally, it assesses performance metrics, acknowledges inherent limitations, and details the types of attacks that can be mitigated through passwordless techniques, while highlighting novel solutions that have been proposed. Security control remains a cornerstone of IT security [101] and password has been used for a long time as method of control. However, transitioning to passwordless authentication offers significant security enhancements by eliminating reliance on traditional passwords. This research aims to provide a holistic understanding of various passwordless authentication techniques and schemes. It uncovers numerous advantages, including improvements in security, reliability, performance efficiency, privacy protection, mutual authentication, flexibility, scalability, real-time monitoring, decentralization, and fairness. These benefits underscore the transformative potential of passwordless technology in enhancing security and privacy across sectors such as healthcare, education, the public sector, and communication.

Despite the clear benefits, it is critical to acknowledge the limitations and challenges associated with passwordless authentication. These challenges include issues related to reliability, usability, integration, compatibility, computational complexity, and implementation. Overcoming these obstacles is essential to facilitate the widespread adoption of passwordless authentication techniques. Future research must focus on addressing these challenges to promote the successful implementation of secure authentication methods in the IT landscape. Key areas for future research include efficiency enhancements to streamline processes and improve usability, practical real-world implementation to validate scalability and resilience, and scalability improvements for seamless integration into diverse IT environments. Ongoing security advancements are essential to counter evolving threats, while integrating AI and machine learning can enhance adaptability and real-time threat detection. Additionally, design improvements in authentication interfaces are crucial for user-friendliness and widespread adoption.

These insights serve as a roadmap to address current challenges and advance passwordless authentication across various sectors. As digital transformation continues to integrate deeply into everyday life, it has also created significant opportunities for cybercrime to thrive [102]. particularly through attacks on online transactions. Many of these security challenges arise from vulnerabilities in online authentication schemes [103]. Thus, seamlessly integrating passwordless technology is essential for enhancing security and privacy across various applications, ensuring its widespread adoption and impact on daily life. Through this review, this paper contributes significantly by analysing advancements, challenges, and opportunities in passwordless authentication, providing a comprehensive understanding of its current state and future directions and we hope these findings will outline the focus and key areas for future works.

REFERENCES

[1] P. R. S. Rajah, O. Dastane, K. A. Bakon, and Z. Johari, "The effect of bad password habits on personal data breach," *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 10, pp. 6950–6960, Oct. 2020, doi: 10.30534/ijeter/2020/538102020.

[2] M. A. A. Kabir and W. Elmedany, "An overview of the present and future of user authentication," in *Proc. 4th IEEE Middle East North Afr. Commun. Conf. (MENACOMM)*, Dec. 2022, pp. 10–17, doi: 10.1109/MENACOMM57252.2022.9998304.

[3] R. Gonzalez, E. Y. Chen, and C. Jackson, "Automated password extraction attack on modern password managers," 2013, *arXiv:1309.1416*.

[4] V. Parmar, H. A. Sanghvi, R. H. Patel, and A. S. Pandya, "A comprehensive study on passwordless authentication," in *Proc. Int. Conf. Sustain. Comput. Data Commun. Syst. (ICSCDS)*, Apr. 2022, pp. 1266–1275, doi: 10.1109/ICSCDS53736.2022.9760934.

[5] M. Campbell, "Putting the passe into passwords: How passwordless technologies are reshaping digital identity," *Computer*, vol. 53, no. 8, pp. 89–93, Aug. 2020, doi: 10.1109/MC.2020.2997278.

[6] H. Feng, J. Guan, H. Li, X. Pan, and Z. Zhao, "FIDO gets verified: A formal analysis of the universal authentication framework protocol," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 5, pp. 4291–4310, Sep. 2023, doi: 10.1109/TDSC.2022.3217259.

[7] I. L. Furuberg and M. Øseth, "From password to passwordless: Exploring user experience obstacles to the adoption of FIDO2 authentication," Master thesis, Dept. Information security and communication technology, Norwegian Univ. Sci. Technol., Trondheim, Norway, 2023, doi: https://hdl.handle.net/11250/3093908.

[8] F. Alqubaisi, A. S. Wazan, L. Ahmad, and D. W. Chadwick, "Should we rush to implement password-less single factor FIDO2 based authentication?" in *Proc. 12th Annu. Undergraduate Res. Conf. Appl. Comput. (URC)*, Apr. 2020, pp. 1–6, doi: 10.1109/URC49805.2020.9099190.

[9] A. Angelogianni, I. Politis, and C. Xenakis, "How many FIDO protocols are needed? Surveying the design, security and market perspectives," 2021, *arXiv:2107.00577*.

[10] M. Kepkowski, M. Machulak, I. Wood, and D. Kaafar, "Challenges with passwordless FIDO2 in an enterprise setting: A usability study," 2023, *arXiv:2308.08096*.

[11] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Z. Fardi, and S. Samad, "Authentication systems: A literature review and classification," *Telematics Informat.*, vol. 35, no. 5, pp. 1491–1511, Aug. 2018, doi: 10.1016/j.tele.2018.03.018.

[12] N. H. Kamarudin, N. H. S. Suhaimi, F. A. N. Rashid, M. N. A. Khalid, and F. Mohd Ali, "Exploring authentication paradigms in the Internet of Things: A comprehensive scoping review," *Symmetry*, vol. 16, no. 2, p. 171, Feb. 2024, doi: 10.3390/sym16020171.

[13] R. M. Jyothi and N. Jeyanthi, "A review of modern authentication methods in digital systems," in *Proc. Annu. Int. Conf. Emerg. Res. Areas: Int. Conf. Intell. Syst. (AICERA/ICIS)*, Nov. 2023, pp. 1–6, doi: 10.1109/AICERA/ICIS59538.2023.10420169.

[14] J. Glöckler, J. Sedlmeir, M. Frank, and G. Fridgen, "A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity," *Bus. Inf. Syst. Eng.*, vol. 66, no. 4, pp. 421–440, Sep. 2023, doi: 10.1007/s12599-023-00830-x.

[15] D. Köhler, E. Klieme, M. Kreuseler, F. Cheng, and C. Meinel, "Assessment of remote biometric authentication systems: Another take on the quest to replace passwords," in *Proc. IEEE 5th Int. Conf. Cryptography, Secur. Privacy (CSP)*, Jan. 2021, pp. 22–31, doi: 10.1109/CSP51677.2021.9357504.

[16] Y. Yu, Q. Niu, X. Li, J. Xue, W. Liu, and D. Lin, "A review of fingerprint sensors: Mechanism, characteristics, and applications," *Micromachines*, vol. 14, no. 6, p. 1253, Jun. 2023, doi: 10.3390/mi14061253.

[17] K. Bicakci and Y. Uzunay, "Is FIDO2 passwordless authentication a hype or for real: A position paper," in *Proc. 15th Int. Conf. Inf. Secur. Cryptography (ISCTURKEY)*, Oct. 2022, pp. 68–73, doi: 10.1109/ISCTURKEY56345.2022.9931832.

[18] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Systematic Rev.*, vol. 10, no. 1, p. 372, Dec. 2021, doi: 10.1186/s13643-021-01626-4.

[19] A. Rashik and C. V. Priya, "A secure application of multi-biometric recognition and QR coding system," in *Proc. Int. Conf. Innov. Trends Inf. Technol. (ICITIIT)*, Feb. 2022, pp. 1–6, doi: 10.1109/ICITIIT54346.2022.9744156.

[20] S. Lambert, "A usability study of FIDO2 hardware tokens on mobile devices," Master's thesis, Dept. Master Science, Brigham Young Univ., Provo, UT, USA, 2022. [Online]. Available: http://hdl.lib.byu.edu/1877/etd12619

[21] B. Rasmussen, "A usability study of FIDO2 roaming software tokens as a password replacement password replacement," Master's thesis, Dept. Computer Science, Brigham Young Univ., Provo, UT, USA, 2021. [Online]. Available: https://scholarsarchive.byu.edu/etd/9227

[22] F. Vega, "An empirical study on the usability and security of two-factor authentication," Master's thesis, Dept. Computer Science, California State Univ., Los Angeles, CA, USA, 2022. [Online]. Available: http://hdl.handle.net/20.500.12741/rep

[23] J. Haddad, N. Pitropakis, C. Chrysoulas, M. Lemoudden, and W. J. Buchanan, "Attacking windows hello for business: Is it what we were promised?" *Cryptography*, vol. 7, no. 1, p. 9, Feb. 2023, doi: 10.3390/cryptography7010009.

[24] D. Progonov, V. Cherniakova, P. Kolesnichenko, and A. Oliynyk, "Behavior-based user authentication on mobile devices in various usage contexts," *EURASIP J. Inf. Secur.*, vol. 2022, no. 1, p. 6, Sep. 2022, doi: 10.1186/s13635-022-00132-x.

[25] A. H. Han and D. H. Lee, "Detecting risky authentication using the OpenID connect token exchange time," *Sensors*, vol. 23, no. 19, p. 8256, Oct. 2023, doi: 10.3390/s23198256.

[26] A. V. Grammatopoulos, "FIDO2/WebAuthn implementation and analysis in terms of PSD2," Master's thesis, Dept. Digital Systems, Univ. Piraeus, Piraeus, Greece, 2022.

[27] H. A. Rahman and N. Yulianti, "Implementation a passwordless and multi factor authentication (MFA) mechanism for enhancing login security in Android applications," in *Proc. Int. Conf. Informat., Multimedia, Cyber Informations Syst. (ICIMCIS)*, Nov. 2023, pp. 206–211, doi: 10.1109/icimcis60089.2023.10348624.

[28] M. Ioannis, "Integration of OpenID connect with FIDO UAF for Android environments," Master's thesis, Dept. Digital Systems, Univ. Piraeus, Piraeus, Greece, 2021, doi: 10.26267/unipi_dione/1518.

[29] M. Jubur, "On the security and usability of new paradigms of Web authentication," Doctoral dissertation, Dept. Computer Science, Univ. Alabama at Birmingham, Birmingham, AL, USA, 2021.

[30] I. S. Matiushin and V. V. Korkhov, "Passwordless authentication using magic link technology," in *Proc. CEUR Workshop*, 2021, pp. 434–438.

[31] Y. Huang, B. Fu, N. Peng, Y. Ba, X. Liu, and S. Zhang, "RFID authentication system based on user biometric information," *Appl. Sci.*, vol. 12, no. 24, p. 12865, Dec. 2022, doi: 10.3390/app122412865.

[32] T. Mokoena and D. Sabatta, "User classification by keystroke dynamics using text retrieval methods," in *Proc. Int. SAUPEC/RobMech/PRASA Conf.*, Jan. 2020, pp. 1–6, doi: 10.1109/SAUPEC/RobMech/PRASA48453.2020.9040956.

[33] J. Liu, X. Zou, J. Han, F. Lin, and K. Ren, "BioDraw: Reliable multi-factor user authentication with one single finger swipe," in *Proc. IEEE/ACM 28th Int. Symp. Quality Service (IWQoS)*, Jun. 2020, pp. 1–10, doi: 10.1109/IWQoS49365.2020.9212855.

[34] E. Dimitrova, D. Dimitrova, V. Dimitrov, and V. Trifonov, "Contemporary authentication access approach for high security information systems," in *Proc. 56th Int. Sci. Conf. Inf., Commun. Energy Syst. Technol. (ICEST)*, Jun. 2021, pp. 37–40, doi: 10.1109/ICEST52640.2021.9483496.

[35] Y. B. W. Piugie, J. Di Manno, C. Rosenberger, and C. Charrier, "Keystroke dynamics based user authentication using deep learning neural networks," in *Proc. Int. Conf. Cyberworlds (CW)*, Sep. 2022, pp. 220–227, doi: 10.1109/CW55638.2022.00052.

[36] E. Dauterman, D. Lin, H. Corrigan-Gibbs, and D. Mazières, "Accountable authentication with privacy protection: The larch system for universal login," 2023, *arXiv:2305.19241*.

[37] A. H. Al-Rashid, "Biometrics authentication: Issues and solutions," Doctoral dissertation, Dept. Faculty Science Engineering, Hamad Bin Khalifa Univ., Ar-Rayyan, Qatar, 2020.

[38] Z. I. Khan and V. K. Shandilya, "Enhanced recognition based image authentication scheme to save system time & memory," in *Proc. IEEE Bombay Sect. Signature Conf. (IBSSC)*, Dec. 2020, pp. 84–90, doi: 10.1109/IBSSC51096.2020.9332183.

[39] Y. Omori and T. Yamashita, "Extended inter-device digital rights sharing and transfer based on device-owner equality verification using homomorphic encryption," *IEICE Trans. Inf. Syst.*, vol. 103, no. 6, pp. 1339–1354, Jun. 2020, doi: 10.1587/transinf.2019edp7163.

[40] C. Guo, Q. Cai, Q. Wang, and J. Lin, "Extending registration and authentication processes of FIDO2 external authenticator with QR codes," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 518–529, doi: 10.1109/TrustCom50675.2020.00076.

[41] D. Lohr and O. V. Komogortsev, "Eye know you too: Toward viable end-to-end eye movement biometrics for user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3151–3164, 2022, doi: 10.1109/TIFS.2022.3201369.

[42] W.-Z. Yeoh, M. Kepkowski, G. Heide, D. Kaafar, and L. Hanzlik, "Fast IDentity online with anonymous credentials (FIDO-AC)," 2023, *arXiv:2305.16758*.

[43] E. Klieme, J. Wilke, N. van Dornick, and C. Meinel, "FIDOnuous: A FIDO2/WebAuthn extension to support continuous Web authentication," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1857–1867, doi: 10.1109/TrustCom50675.2020.00254.

[44] M. A. Alqarni, S. H. Chauhdary, M. N. Malik, M. Ehatisham-Ul-Haq, and M. A. Azam, "Identifying smartphone users based on how they interact with their phones," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, p. 7, Dec. 2020, doi: 10.1186/s13673-020-0212-7.

[45] A. Galli, G. Giorgi, and C. Narduzzi, "Individual recognition by Gaussian ECG features," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. (I2MTC)*, May 2020, pp. 1–5, doi: 10.1109/I2MTC43012.2020.9129092.

[46] S. Ghorbani 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," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 268–285, doi: 10.1109/sp40000.2020.00047.

[47] L. Lassak, M. Golla, A. Hildebrandt, and B. Ur, "'It's stored, hopefully, on an encrypted server': Mitigating users' misconceptions about FIDO2 biometric WebAuthn," in *Proc. 30th USENIX Secur. Symp. (USENIX Secur.)*, 2021, pp. 91–108. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/lassak

[48] J. Conners, C. Devenport, S. Derbidge, N. Farnsworth, K. Gates, S. Lambert, C. McClain, P. Nichols, and D. Zappala, "Let's authenticate: Automated certificates for user authentication," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2022, pp. 1–11, doi: 10.14722/ndss.2022.24272.

[49] K. Bicakci and A. Drobi, "QRAuth: A secure and accessible Web authentication alternative to FIDO2," in *Proc. 16th Int. Conf. Inf. Secur. Cryptol. (ISCTürkiye)*, Oct. 2023, pp. 1–7, doi: 10.1109/isc-trkiye61151.2023.10336164.

[50] J. Fietkau, S. M. Zahra, and M. Hartung, "Secure authentication for everyone! Enabling 2nd-factor authentication under real-world constraints," in *Proc. 2nd Int. Symp. Secur. Comput. Inf. Sci.* Cham, Switzerland: Springer, 2022, pp. 89–101, doi: 10.1007/978-3-031-09357-9_8.

[51] Y. Sun. (2021). *Security and Privacy Solutions for Camera and Camera Based Authentication*. Accessed: Jun. 6, 2024. [Online]. Available: https://etda.libraries.psu.edu/catalog/21161yus160

[52] T. Laing, E. Marin, M. D. Ryan, J. Schiffman, and G. Wattiau, "Symbolon: Enabling flexible multi-device-based user authentication," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Jun. 2022, pp. 1–12, doi: 10.1109/DSC54232.2022.9888854.

[53] A. Mitra, A. Ghosh, and S. C. Sethuraman, "TUSH-key: Transferable user secrets on hardware key," 2023, *arXiv:2307.07484*.

[54] K. Owens, O. Anise, and A. Krauss, "User perceptions of the usability and security of smartphones as FIDO2 roaming authenticators," in *Proc. 17th Symp. Usable Privacy Secur.*, 2021, pp. 57–76. Accessed: Jun. 6, 2024. [Online]. Available: https://www.usenix.org/conference/soups2021/presentation/owens

[55] F. M. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. Dürmuth, "'You still use the password after all'—Exploring FIDO2 security keys in a small company," in *Proc. 16th Symp. Usable Privacy Secur.*, 2020, pp. 19–35. Accessed: Jun. 6, 2024. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/farke

[56] T. Hackenjos, B. Wagner, J. Herr, J. Rill, M. Wehmer, N. Goerke, and I. Baumgart, "FIDO2 with two displays-or how to protect security-critical Web transactions against malware attacks," 2022, *arXiv:2206.13358*.

[57] P. Muzikant and J. Hajný, "Integrating smart card authentication to Web applications," in *Proc. 14th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Oct. 2022, pp. 90–95, doi: 10.1109/ICUMT57764.2022.9943364.

[58] S. Chakraborty, R. Kundu, S. Paramanik, A. Kumari, and U. Mukherjee, "Realtime authentication using 3D password," in *Proc. IEEE Int. Power Renew. Energy Conf. (IPRECON)*, Dec. 2022, pp. 1–5, doi: 10.1109/IPRECON55716.2022.10059508.

[59] A. Mahnamfar, K. Bicakci, and Y. Uzunay, "ROSTAM: A passwordless Web single sign-on solution mitigating server breaches and integrating credential manager and federated identity systems," 2023, *arXiv:2310.05222*.

[60] B. Boi, M. De Santis, and C. Esposito, "Self-sovereign identity (SSI) attribute-based Web authentication," in *Proc. 20th Int. Conf. Secur. Cryptography*, 2023, pp. 758–763, doi: 10.5220/0012121400003555.

[61] S. Ferdous, A. Ionita, and W. Prinz, "SSI4Web: A self-sovereign identity (SSI) framework for the Web," in *Proc. Int. Congr. Blockchain Appl.*, 2022, pp. 366–379, doi: 10.1007/978-3-031-21229-1_34.

[62] C. Wu, K. He, J. Chen, R. Du, and Y. Xiang, "CaIAuth: Context-aware implicit authentication when the screen is awake," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11420–11430, Dec. 2020, doi: 10.1109/JIOT.2020.3006870.

[63] W. Cheung and S. Vhaduri, "Continuous authentication of wearable device users from heart rate, gait, and breathing data," in *Proc. 8th IEEE RAS/EMBS Int. Conf. Biomed. Robot. Biomechatronics (BioRob)*, Nov. 2020, pp. 587–592, doi: 10.1109/BioRob49111.2020.9224356.

[64] S. Vhaduri, S. V. Dibbo, and W. Cheung, "HIAuth: A hierarchical implicit authentication system for IoT wearables using multiple biometrics," *IEEE Access*, vol. 9, pp. 116395–116406, 2021, doi: 10.1109/ACCESS.2021.3105481.

[65] Y. Ming, P. Yang, H. Mahdikhani, and R. Lu, "A secure one-to-many authentication and key agreement scheme for industrial IoT," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2225–2236, Jun. 2023, doi: 10.1109/JSYST.2022.3209868.

[66] K. A. P. S. Parameswaran, M. A. Majid, H. Ajra, and M. S. Islam, "Fingerprint authentication-based traffic offence control and enforcement system on smart mobile devices for smart city," in *Proc. Int. Conf. Intell. Technol., Syst. Service Internet Everything (ITSS-IoE)*, Dec. 2022, pp. 1–6, doi: 10.1109/ITSS-IoE56359.2022.9990947.

[67] L. Mainetti, P. Panarese, and R. Vergallo, "WoX+: A meta-model-driven approach to mine user habits and provide continuous authentication in the smart city," *Sensors*, vol. 22, no. 18, p. 6980, Sep. 2022, doi: 10.3390/s22186980.

[68] C. Liu, L. Yang, L. Ma, L. Shi, X. Hu, W. Cao, and J. Zhang, "PEBIID: Privacy-preserving and efficient biometric identification for IoV DApp," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Sep. 2021, pp. 63–72, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00023.

[69] H. Sikarwar and D. Das, "A novel MAC-based authentication scheme (NoMAS) for Internet of Vehicles (IoV)," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 4904–4916, May 2023, doi: 10.1109/TITS.2023.3242291.

[70] A. T. Merrill, "Detecting and correcting client-side ballot manipulation in Internet voting systems acknowledgements," Ph.D. thesis, Dept. Master Science Computer Science, New Mex. Inst. Mining Technol., Socorro, NM, USA, 2021.

[71] H. H. Al-Ameri and S. Ayvaz, "A blockchain-based secure mutual authentication system for E-government services," in *Proc. 3rd Int. Sci. Conf. Eng. Sci. (ISCES)*, May 2023, pp. 19–24, doi: 10.1109/isces58193.2023.10311497.

[72] R. Laborde, A. Oglaza, S. Wazan, F. Barrere, A. Benzekri, D. W. Chadwick, and R. Venant, "A user-centric identity management framework based on the W3C verifiable credentials and the FIDO universal authentication framework," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–8. [Online]. Available: https://sovrin.org

[73] S. Ranise, G. Sciarretta, and A. Tomasi, "Enroll, and authentication will follow: EID-based enrollment for a customized, secure, and frictionless authentication experience," in *Proc. 12th Int. Symp. Found. Pract. Secur.*, in Lecture Notes in Computer Science, vol. 12056. Cham, Switzerland: Springer, 2020, pp. 156–171, doi: 10.1007/978-3-030-45371-8.

[74] W.-H. Lin, G.-Y. Yang, and K.-H. Yeh, "Integrating FIDO authentication with new digital identity in Taiwan," in *Proc. IEEE 11th Global Conf. Consum. Electron. (GCCE)*, Oct. 2022, pp. 311–312, doi: 10.1109/GCCE56475.2022.10014031.

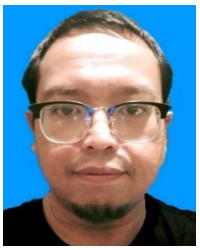
[75] M. Keil, P. Markert, and M. Dürmuth, "'It's just a lot of prerequisites': A user perception and usability analysis of the German ID card as a FIDO2 authenticator," in *Proc. Eur. Symp. Usable Secur.*, Sep. 2022, pp. 172–188, doi: 10.1145/3549015.3554208.

[76] A. J. Y. Aldarwish, K. K. Patel, A. A. Yassin, K. Patel, A. A. Yassin, and A. A. Yaseen, "Virtual SmartCards-based authentication in healthcare systems and applications," *Int. J. Comput. Inf. Syst. Ind. Manag. Appl.*, vol. 15, pp. 522–530, Sep. 2023. [Online]. Available: https://www.mirlabs.net/ijcisim/index.html

[77] T.-V. Le, C.-F. Lu, C.-L. Hsu, T. K. Do, Y.-F. Chou, and W.-C. Wei, "A novel three-factor authentication protocol for multiple service providers in 6G-aided intelligent healthcare systems," *IEEE Access*, vol. 10, pp. 28975–28990, 2022, doi: 10.1109/ACCESS.2022.3158756.

[78] H. Kim, D. Lee, and J. Ryou, "User authentication method using FIDO based password management for smart energy environment," in *Proc. Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2020, pp. 707–710, doi: 10.1109/ICDMW51313.2020.00100.

[79] M. Rivera-Dourado, M. Gestal, A. Pazos, and J. Vázquez-Naya, "A novel protocol using captive portals for FIDO2 network authentication," *Appl. Sci.*, vol. 14, no. 9, p. 3610, Apr. 2024, doi: 10.3390/app14093610.
[80] I. Al Rassan and H. Alajlan, "Approach of migrating SAAS applications to password-less authentication," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2022, pp. 1341–1345, doi: 10.1109/csci58124.2022.00241.
[81] S. P. Rao and A. Bakas, "Authenticating mobile users to public Internet commodity services using SIM technology," in *Proc. 16th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, May 2023, pp. 151–162, doi: 10.1145/3558482.3590181.
[82] I. Gordin, A. Graur, S. Vlad, and C. I. Adomnitei, "Moving forward passwordless authentication: Challenges and implementations for the private cloud," in *Proc. 20th RoEduNet Conference: Netw. Educ. Res. (RoEduNet)*, Nov. 2021, pp. 1–5, doi: 10.1109/RoEduNet54112.2021.9638271.
[83] E. Huseynov, "Passwordless VPN using FIDO2 security keys: Modern authentication security for legacy VPN systems," in *Proc. 4th Int. Conf. Data Intell. Secur. (ICDIS)*, Aug. 2022, pp. 453–455, doi: 10.1109/ICDIS55630.2022.00075.
[84] C. Shi, J. Liu, N. Borodinov, B. Leao, and Y. Chen, "Towards environment-independent behavior-based user authentication using WiFi," in *Proc. IEEE 17th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Dec. 2020, pp. 666–674, doi: 10.1109/MASS50613.2020.00086.
[85] A. M. Mostafa, M. Ezz, M. K. Elbashir, M. Alruily, E. Hamouda, M. Alsarhani, and W. Said, "Strengthening cloud security: An innovative multi-factor multi-layer authentication framework for cloud user authentication," *Appl. Sci.*, vol. 13, no. 19, p. 10871, Sep. 2023, doi: 10.3390/app131910871.
[86] S. Lee, H. Yeo, and M. Kang, "Biometric authentication sensor with an encryption module for prevention of h/w hacking in digital custody services," *Int. J. Smart Sens. Intell. Syst.*, vol. 16, no. 1, pp. 1–16, Jan. 2023, doi: 10.2478/ijssis-2023-0004.
[87] S. C. Sethuraman, A. Mitra, K.-C. Li, A. Ghosh, M. Gopinath, and N. Sukhija, "Loki: A physical security key compatible IoT based lock for protecting physical assets," *IEEE Access*, vol. 10, pp. 112721–112730, 2022, doi: 10.1109/ACCESS.2022.3216665.
[88] J. Lio and T. Okada, "An experimental trial of a novel ticketing system using biometrics," in *Proc. Adv. Artif. Intell., Softw. Syst. Eng.* Cham, Switzerland: Springer, 2019, pp. 499–507. [Online]. Available: http://www.springer.com/series/11156
[89] G. Ali, M. A. Dida, and A. E. Sam, "A secure and efficient multi-factor authentication algorithm for mobile money applications," *Future Internet*, vol. 13, no. 12, p. 299, Nov. 2021, doi: 10.3390/fi13120299.
[90] I. Tilloo and S. Bhingarkar, "Cardless cash withdrawal using palm vein technology," in *Proc. Int. Conf. Futuristic Technol. (INCOFT)*, Nov. 2022, pp. 1–5, doi: 10.1109/INCOFT55651.2022.10094450.
[91] R. Laborde, A. Oglaza, S. Wazan, F. Barrère, A. Benzekri, D. W. Chadwick, and R. Venant, "Know your customer: Opening a new bank account online using UAAF," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–2, doi: 10.1109/CCNC46108.2020.9045148.
[92] Z. Chen, H. Cai, L. Jiang, W. Zou, W. Zhu, and X. Fei, "Keystroke dynamics based user authentication and its application in online examination," in *Proc. IEEE 24th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2021, pp. 649–654, doi: 10.1109/CSCWD49262.2021.9437721.
[93] J. P. da Paula Manteigueiro, D. P. A. C. Co-Orientador, and D. C. M. C. S. Barrico. (2020). *Authentication and Identity Management for the EPOS Project*. Accessed: Jun. 6, 2024. [Online]. Available: https://www.proquest.com/docview/2586971568?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses
[94] V. Baneş, C. Ravariu, B. Appasani, and A. Srinivasulu, "A novel two-factor authentication scheme for increased security in accessing the moodle E-learning platform," *Appl. Sci.*, vol. 13, no. 17, p. 9675, Aug. 2023, doi: 10.3390/app13179675.
[95] E. R. de Mello, M. S. Wangham, S. B. Loli, C. E. da Silva, G. C. da Silva, S. A. de Chaves, and B. B. Loli, "Multi-factor authentication for shibboleth identity providers," *J. Internet Services Appl.*, vol. 11, no. 1, pp. 1–21, Dec. 2020, doi: 10.1186/s13174-020-00128-1.
[96] J. Li. (2023). *Empowering Security and Privacy-Preserving Interactions for Smart Device Users*. Accessed: Jun. 6, 2024. [Online]. Available: https://search.library.wisc.edu/digital/AEBWKIRKET37KC82
[97] S. Chakkaravarthy Sethuraman, A. Mitra, A. Ghosh, G. Galada, and A. Subramanian, "MetaSecure: A passwordless authentication for the metaverse," 2023, *arXiv:2301.01770*.
[98] M. Dammak, S. Aroua, S. M. Senouci, Y. Ghamri-Doudane, G. Suciu, M.-A. Sachian, R. Roscaneanu, I. Ozkan, and M. O. Gungor, "A secure and interoperable platform for privacy protection in the smart hotel context," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Oct. 2020, pp. 1–6, doi: 10.1109/GIIS50753.2020.9248483.
[99] D. Boshoff, R. Nkrow, and G. P. Hancke, "Knock-to-enter authentication: A rhythm-based smartphone authentication mechanism," in *Proc. 49th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2023, pp. 1–6, doi: 10.1109/iecon51785.2023.10312590.
[100] M. K. Hasan, Z. Weichen, N. Safie, F. R. A. Ahmed, and T. M. Ghazal, "A survey on key agreement and authentication protocol for Internet of Things application," *IEEE Access*, vol. 12, pp. 61642–61666, 2024, doi: 10.1109/ACCESS.2024.3393567.
[101] N. Musa, "A conceptual framework of IT security governance and internal controls," in *Proc. Cyber Resilience Conf. (CRC)*, Nov. 2018, pp. 1–4, doi: 10.1109/CR.2018.8626831.
[102] K. Osman and T. Q. Feng, "Validation of individual identification through decision tree packet header profiling," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 11, no. 2, pp. 97–111, Dec. 2022, doi: 10.17576/apjitm-2022-1102-08.
[103] M. A. Hassan and Z. Shukur, "A systematic review of user authentication security in electronic payment system," in *Proc. Int. Conf. Data Sci. Appl.*, in Lecture Notes in Networks and Systems, Jan. 2023, pp. 121–138, doi: 10.1007/978-981-19-6631-6_10.



MOHD IMRAN MD YUSOP received the bachelor's degree in information system engineering from the Mara University of Technology (UiTM). He is currently pursuing his study with Cybersecurity Center, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. His career started as an Intern with Sun Microsystems, from 2006 to 2007. From 2007 to 2009, he was an Engineer with Time Dot Com and U Mobile handling and implementing telecommunication infrastructure applications planning and operations. From 2009 to 2023, he was assigned to various ministries and agencies, including the Ministry of Education, the Ministry of Higher Education, the Syariah Judiciary Department (JKSM), the National Disaster Management Agency (NADMA), and the Prime Minister Office (PMO) managing and overseeing various government projects ranging from application, networks, data center, security, and enterprise architecture. He is currently a Senior Information Technology Officer attached to the National Digital Agency (JDN).

NAZHATUL HAFIZAH KAMARUDIN (Member, IEEE) received the Bachelor of Engineering degree in electrical engineering and the Master of Engineering degree in wireless security from the Stevens Institute of Technology, NJ, USA, and the Ph.D. degree in electrical engineering with a specialization in security and cryptography from UiTM Shah Alam, in 2019. She is currently a Senior Lecturer with the Centre for Cybersecurity, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. Prior to her current role, she was an Assistant Professor with UCSI University and a Lecturer with the Infrastructure University of Kuala Lumpur (IUKL). Her research interests include authentication, network security, information security, and artificial intelligence. She is a Graduate Member of the Board of Engineers Malaysia (BEM). She is a Professional Technologist certified by Malaysian Board of Technologists (MBOT).

NUR HANIS SABRINA SUHAIMI (Member, IEEE) received the B.Eng. degree in communication engineering from International Islamic University, Malaysia (IIUM), Selangor, Malaysia, in 2013, the M.Sc. degree in remote sensing and GIS from Universiti Putra Malaysia (UPM), Selangor, in 2015, and the Ph.D. degree in engineering from IIUM, in 2023. Currently, she is a Senior Lecturer with the Cybersecurity Center, Faculty of Technology Sciences Information (FTSM), Universiti Kebangsaan Malaysia (UKM). She has nine years of experiences as a Research Officer with the Division of Maritime Technology, Science and Technology Research Institute for Defence (STRIDE), and one year of experience as a Software Engineer with Sony EMCS (Malaysia) Sdn Bhd, Bangi, Selangor. She has published research papers in national and international journals as well as in conference proceedings. Her research interests include wireless and mobile networks, data communication, network and communication security, microwave propagation technologies, beyond 5G networks, mmWave, and THz communication in cellular and satellite communication studies. She is a committee for the ASEAN Workshop of Information Science and Technology (AWIST), a member of the IEEE Society and BEM, a member of Malaysian Electromagnetic Spectrum Association (MESA), and a Professional Technologist certified by the Malaysian Board of Technologists (MBOT).

MOHAMMAD KAMRUL HASAN (Senior Member, IEEE) received the Doctor of Philosophy degree in electrical and communication engineering from the Faculty of Engineering, International Islamic University, Malaysia, in 2016. He is currently an Associate Professor and the Head of the Network and Communication Technology Research Laboratory, Center for Cyber Security, Universiti Kebangsaan Malaysia (UKM). He is a certified Professional Technologist in Malaysia. He has published more than 300 indexed papers in ranked journals and conference proceedings. He specializes in elements pertaining to cutting-edge information-centric networks, computer networks, data communication and security, mobile network and privacy protection, cyber-physical systems, the industrial IoT, transparent AI, and electric vehicle networks. He is a member of the Institution of Engineering and Technology and the Internet Society. He is an Editorial Member of many prestigious high-impact journals, such as IEEE, IET, Elsevier, Frontier, and MDPI. He served as the Chair for the IEEE Student Branch, from 2014 to 2016. He has actively participated in many events/workshops/trainings for the IEEE Humanity Program. He is the general chair, the co-chair, and a speaker of conferences and workshops for the shake of society and academy knowledge building and sharing and learning.