Optimized Security Authentication Protocols for Network Access Nodes: A Detailed Performance and Vulnerability Assessment

T.N. Ahamed, M.J.A. Sabani and M.S. Shafana

Abstract— As networked access nodes like wireless access points and routers are increasingly used, wireless technology security is becoming increasingly important. These nodes are susceptible to attacks like Man-in-the-Middle (MitM). In order to maintain data integrity and confidentiality and to stop unwanted access, this literature review investigates effective security authentication techniques for these networked access nodes. There is a need for more resilient authentication methods because traditional ones such as those dependent on TCP handshakes and static passwords have shown to be insufficient against complex assaults. New techniques that could improve networked environment security are examined including multi-factor authentication, biometric verification, and dynamic password authentication. Computational overhead and user privacy concerns are two implementation challenges highlighted in the review. The paper also looks at replay, phishing, and impersonation assaults, among other attacks on authentication systems, and evaluates the efficacy of various defenses. Reputable databases like Google Scholar, Scopus, IEEE Xplore, and Springer are the source of current research papers and technical reports for the literature review, limited to works published during the previous five years. The results highlight the significance of implementing a multi-layered authentication strategy incorporating conventional and cutting-edge methods to protect networked access nodes effectively. In order to provide better, more secure, and effective authentication procedures, the assessment ends by pointing out weaknesses in the currently used approaches and suggesting future paths. The goal of this thorough examination is to lay the groundwork for future investigation and advancement in the field of network security, tackling the escalating difficulties brought about by more complex cyberattacks.

Index Terms – **Authentication, Authentication Methods, Access Node, MFA, Network attacks, Security**

I. Introduction

SECURITY is a significant challenge for wireless technologies, as a radio link is susceptible to malicious events in the utilized frequency and bandwidth. In other words, access nodes employed by end users are insecure and form points of attack for Man-in-the-Middle (MitM) on the information shared between the end user and the network. A real and clearly defined chance of an attack on network information exists when connectionless protocols such as User Datagram Protocol (UDP) packets are shared. Alternatively, in the presence of connected protocols such as Transmission Control Protocol (TCP) or Point Protocol (PPP), there is a window of attack because the completion hand-shaking features provide impact produced amongst packets that are not precisely in order [1].

Authentication mechanisms have been proposed to thwart man-in-the-middle security attacks on connections within wired technologies. Primarily, TCP or PPP protocols have utilized a three-way Hand-shaking mechanism to secure connections. This provides a significant avenue of attack attempt between the requester and acceding hosts, leaving all connections unprotected for one request/accept packet exchange. Even though damage cannot be enacted on a connection, an attacker can collect sensible information or impersonate luggage or destination ships as if both acceding hosts have authorized the requests. Combined with firewalls that keep logs of all previous packets over a period of time, the chance of recreating attacks is efficacious, indicating that both would be better attacks [2]. Authentication solutions tail-bound attempts per user or by requested ports, reflecting a non-convenient resolution.

A. Scope And Objectives of the Literature Review

Different aspects of the problem of providing an efficient security authentication method for networked access nodes have been researched and attempted through several solutions, which were and are still being further developed and optimized, starting from early styles of password-based user access authentication up to new hardware-based authentication tokens. This literature review will present solutions in several available architectures and their drawbacks in providing an efficient authentication method.

T.N. Ahamed is a graduate from Department of Information and Communication Technology, South Eastern University of Sri Lanka, Oluvil, Sri Lanka.
(Email: nuskyahamed@seu.ac.lk)

M.J.A. Sabani is a Senior Lecturer attached to the Department of Information and Communication Technology, South Eastern University of Sri Lanka, Oluvil, Sri Lanka.
(Email: mjasabani@seu.ac.lk)

M.S. Shafana is a Senior Lecturer attached to the Department of Information and Communication Technology, South Eastern University of Sri Lanka, Oluvil, Sri Lanka.
(Email: zainashareef@seu.ac.lk)

ISSN: 2961-5992

Further, a completely new paradigm approach to the problem would also be presented and justified.

The review will remain at a high level of abstraction, presenting only the general ideas of different approaches to the problem and introducing a new proposal without going into detailed research and analysis of components of the systems developed. Network security and control access to database data are as crucial as physically securing the server. A basic method for verifying users and providing them with access control privileges typically involves using a username and password combination.

As the usage of IT has continued to grow, the computer user population is also growing, and their knowledge levels are very much diversified. To complicate things further, with the development of "Hackeries" and computer crimes, the question of security is now even more complicated. So many hacker tools are available for invading privacy and stealing data from computers that limiting or controlling unauthorized access to computers or other data storage devices is challenging. In the past, attempts were made to prevent unauthorized access to devices by implementing locks on the physical access level. However, this is still an open issue at higher access levels vis-à-vis the operating system. As a dynamic environment and accessibility to a vast data collection are becoming the norm, developing better and more secure systems for access control and programming interfaces for authenticated trusted programs is mandatory.

II. Methodology

This literature review explains how authentication is used in Networked Access Nodes. Moreover, this review aimed to determine the problems and day-to-day attacks related to authentication.

Various authentication methods and issues related to existing authentication mechanisms are used in security and finally proposed with some accepted authentication mechanisms. This documentation searches for more research papers, conference papers and literature reviews here. Most of those resources were found in Google Scholar, Scopus, IEEE Explore, Web of Science, and Springer databases. Using those databases, one can get the most reliable resources and the most relevant ideas, methods, techniques and updated details from those reliable resources. Here, we have only studied Authentication Methods within the past five years to develop this review paper we have gone through systematic inclusion and exclusion criteria which allows us to make a successful paper on the appropriate heading. Table I shows the criteria which we have imposed in our review paper.

Table I
Inclusion & Exclusion Criteria

Criteria type	Description	Notes
Inclusion	journal articles, book chapters, and conference proceedings that have undergone peer review.	To be included, the articles need to meet all the inclusion criteria.
	Relevance of topic: Security Authentication	
	Relevance of topic: Comprehensive Analysis	
	Relevance of topic: Network Access Nodes	To be included, the articles need to meet all inclusion standards.
	In the language of English	
Exclusion	journal articles, book chapters, and conference proceedings that have not undergone peer review	The article would be excluded if any exclusion criteria were satisfied.
	Not Security Authentication, but irrelevant topics	
	Irrelevant topics: simulations	
	Studying stakeholder views of authentication is an irrelevant topic.	
	Topics irrelevant: researching Network Access Nodes	
	Subjects irrelevant: unrelated to Authentication or Security	
	Not in the English language	

III. Discussion

In order to provide a protected flow of information in a potentially hostile environment, security stands out as the primary issue. This aim can be implemented through the three pillars of the CIA triad, which are availability, secrecy, and integrity, as stated in [3]. The CIA triad security model, commonly depicted as a triangle, entails the integration of the three tenets into a unified system to guarantee a safe IT infrastructure inside an enterprise.

Confidentiality, being unavailable to unauthorized individuals or processes, is the attribute of confidentiality concerning data, services, or resources stored on computer systems. Applying symmetrical or asymmetric cryptographic algorithms, access control lists, or ACLs can guarantee data secrecy.

Integrity is the integrity of preserving the correctness of data, services, or resources of information systems during transmission, processing, or storage and guarding against unauthorized alteration. Access control lists, or ACLs, hash cryptography function values, backup procedures, and the configuration of suitable redundant systems are some methods that can be used to achieve data integrity.

Information systems' availability information, services, and resources are available when they are promptly made available to authorized individuals or processes and have

ISSN: 2961-5992

complete fault tolerance, allowing for task balancing in the case of a security incident or natural disaster. Fault-tolerant technologies can increase the availability of the data already in the system. These technologies include simple virtualized or hybrid RAID storage, represented by hardware devices that protect against data loss and outages, redundant sites, or access control mechanisms.

A. Taxonomy of Authentication Mechanisms

Authentication mechanisms are the rules designated for interaction and verification that the endpoints (laptops, desktops, phones, servers, etc.) or systems use to communicate. The more the user's need to access as many applications as possible increases, the more standards and mechanisms diversify. Selecting the correct authentication mechanism is essential to ensure secure operations and use compatibility. Authentication mechanisms are developed at various functional levels, such as network level, applications, endpoint, device and virtualized level, highlighted in the diagram below [4].

Static Password Authentication

Using a password or PIN as an authenticator is known as static authentication. One type of password, known as a static secret word, is one the client provides as its confirmation secret key to a server; it remains unchanged unless the client requests a change. Below Fig. 1 shows the basic flow of Static Password Authentication methods that we are using day to day life.

Static passwords are often weak and vulnerable to many attacks, such as replay, phishing, social engineering, parcel sniffing, key-logging, and so on, where the attacker can pretend to be the customer and obtain their login credentials.

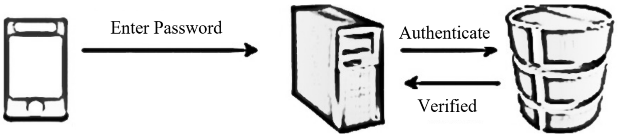

Fig. 1. Static Password Authentication

To strengthen verification, static passwords use a cryptographic hash; nevertheless, this hash is useless against attacks such as keylogging or brute force attacks. Static passwords are still widely used, even though they have many weaknesses. Additionally, using them alone is too dangerous, particularly regarding mobile identity authentication [5].

Dynamic Password Authentication

Among the most popular dynamic password authentication methods is the SMS verification code. Like a static password, the system will need user identity data and a PIN or token the server produces for access authentication [6].

Users must also register and supply a primary key associated with their information, which includes their cell phone number and username, as illustrated in Fig. 2. An SMS with the created password will be sent to the associated cellphone number after the user enters their username and the server confirms that their profile exists. The mobile phone user will then use the generated password to verify their identity. Text messages are used to send SMS authentication codes. Due to its frequent exposure to high-risk threats, this vulnerability exists [7].

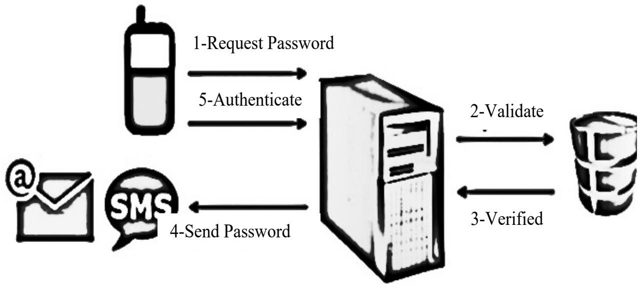

Fig. 2. Dynamic password authentication

Biometric Authentication

High-affirmation biometric features, like fingerprints, iris, face, retina, and hand veins, are utilized to authenticate people. Hackers can get access to traditional authentication methods like passwords and PINs. All security elements are provided via biometric-based authentication, which measures each person's distinct physical and behavioral characteristics. which are used in the biometric authentication process shown in Fig. 3. An individual can also be identified based on his behavioral aspects, such as how he types characters from the keyboard, how he hits the keys, the way he walks or his hand movements [8]

A lot of financial institutions now use biometric authentication as routine practice. For instance, institutions that offer mobile banking apps, such as HSBC and Bank of America, have implemented biometric verification that enables users to safely login with their fingerprint information. Because an attacker would require the user's device in addition to their biometric data to obtain unwanted access, this strategy lessens the likelihood of stolen passwords and phishing attempts.

SMS/ OTP

One of the most widely deployed 2FA methods is SMS. A one-time verification code, typically six digits, is sent via text message to the user's mobile phone. SMS-based authentication is vulnerable at several stages. Mobile networks do not encrypt messages while in transit, allowing attackers to conduct man-in-the-middle attacks. Of particular concern is the well-documented SIM-swapping attack [9] .

One-time passwords (OTPs) sent over SMS are a typical way to establish dynamic password authentication. For example, online banking services use OTPs to validate transactions, which adds an extra degree of security on top of static passwords. In order to prevent replay or phishing attacks, banks such as Chase and Citibank now utilize dynamic passwords for transaction verifications. This enhances the overall security of online banking systems.

PIN

PINs are numerical passwords that are used to verify a user's identity for online banking, mobile devices, and personal computers. Three different kinds of assaults can target them: side-channel, phishing, and smudge attacks. Attackers can use standard methods to determine PINs, infer smudges, and take advantage of touchscreen smudges [10].

QR

Due to its rapid reading and larger storage capacity than traditional barcodes, the QR Code method has gained popularity. A QR code (Quick Response) is a form of matrix barcode that can be scanned by specialized QR barcode readers or smartphones equipped with high-resolution cameras. Quick Response codes are two-dimensional barcodes that help compactly store data. With the widespread usage of smartphones that can scan QR codes, their application is expanding in all spheres of life [11].

Fig. 3. Examples of different biometric traits

Multi-factor authentication - a verification technique

Using more than two categories of credentials. The additional security increases an intruder's difficulty accessing system resources [12]. It uses one or more authentication methods to verify the user's identity during the login process, as follows:

Knowledge factor: An item that the user is aware of, like a password or a simple "secret".

Ownership factor: Refers to something the user possesses, such as a card, smartphone, or other tokens.

The biometric factor: Is the user biometric information, behavioral patterns, or something else entirely.

Employees who access sensitive data remotely over business networks now depend heavily on MFA as a security measure. In order to increase security, businesses like Google and Microsoft have adopted multi-factor authentication (MFA), which requires users to login using two or more methods (such as a password and a one-time code received via SMS or app). In large-scale enterprises, the combination of ownership (one-time code) and knowledge (password) has greatly decreased the incidence of unwanted access. Furthermore, by guaranteeing that only authorized users may access critical resources, multi-factor authentication (MFA) helps to reduce the danger of man-in-the-middle (MitM) attacks in settings such as public Wi-Fi networks.

B. Taxonomy of Authentication Mechanisms

Attackers target networks to gain access to them and obtain valuable information to sell on a black market or fulfill their requirements. This paper will concentrate on various attacks related to authentications among all network attacks. Fig. 4 illustrates the well-formulated taxonomy of attacks on authentications. From these attacks, we will discuss some needed attacks in respective headings.

Attack against Nodes

Node Destruction: Physical destruction (using an electrical surge, physical force, or ammunition) of a node so that it is no longer operable [13].

Node Malfunctioning: Numerous things could cause this, such as malfunctioning sensors, energy loss from overseeing devices, or other denial-of-service attacks.

Node Outage: This kind of attack happens anytime a node stops functioning normally. For instance, if a cluster head fails during routine operations in a heterogeneous network, the WSN protocols must be robust enough to elect new cluster heads and/or provide backup network channels to lessen the detrimental consequences of such node outages.

Attack against Authentication

This category is where attackers forge identities to impersonate authorized users to gain access to the node. [14] defined an authentication attack as a crime where attackers target and exploit the Node authentication process by applying a brute force attack against the PIN. Node authentication attacks are classified into seven categories: impersonation attacks, replay attacks, masquerade attacks, spoofing attacks, social engineering attacks, phishing attacks, and Trojan horse attacks.

Impersonation attacks: This is an attack in which the adversary successfully assumes the identity of a legitimate user or agent to access either the MMS or the information and services of a registered user. People share their PINs with friends and family to perform transactions on their behalf. If an attacker gets access to such a PIN, they can log in to node accounts, perform fraudulent transactions, or change their PIN[15], [16], [17].

Replay attack: This is where an attacker eavesdrops on network communication between the mobile money user and MMS, intercepts the data packets that include the PIN, and then fraudulently delays or resends it to the recipient. This occurs through eavesdropping on mobile communication, and mobile money platforms use SMS to notify mobile money users and agents. The SMS is protected using weak algorithms like the A5, and attackers with scanning software can easily intercept, modify, and resend them [14]. The attacker can misuse the previously exchanged messages between the mobile money user and MMSP to perform the replay attacks.

Masquerade attack: A masquerade attack occurs when an adversary obtains the subscribers' SIM card and PIN and

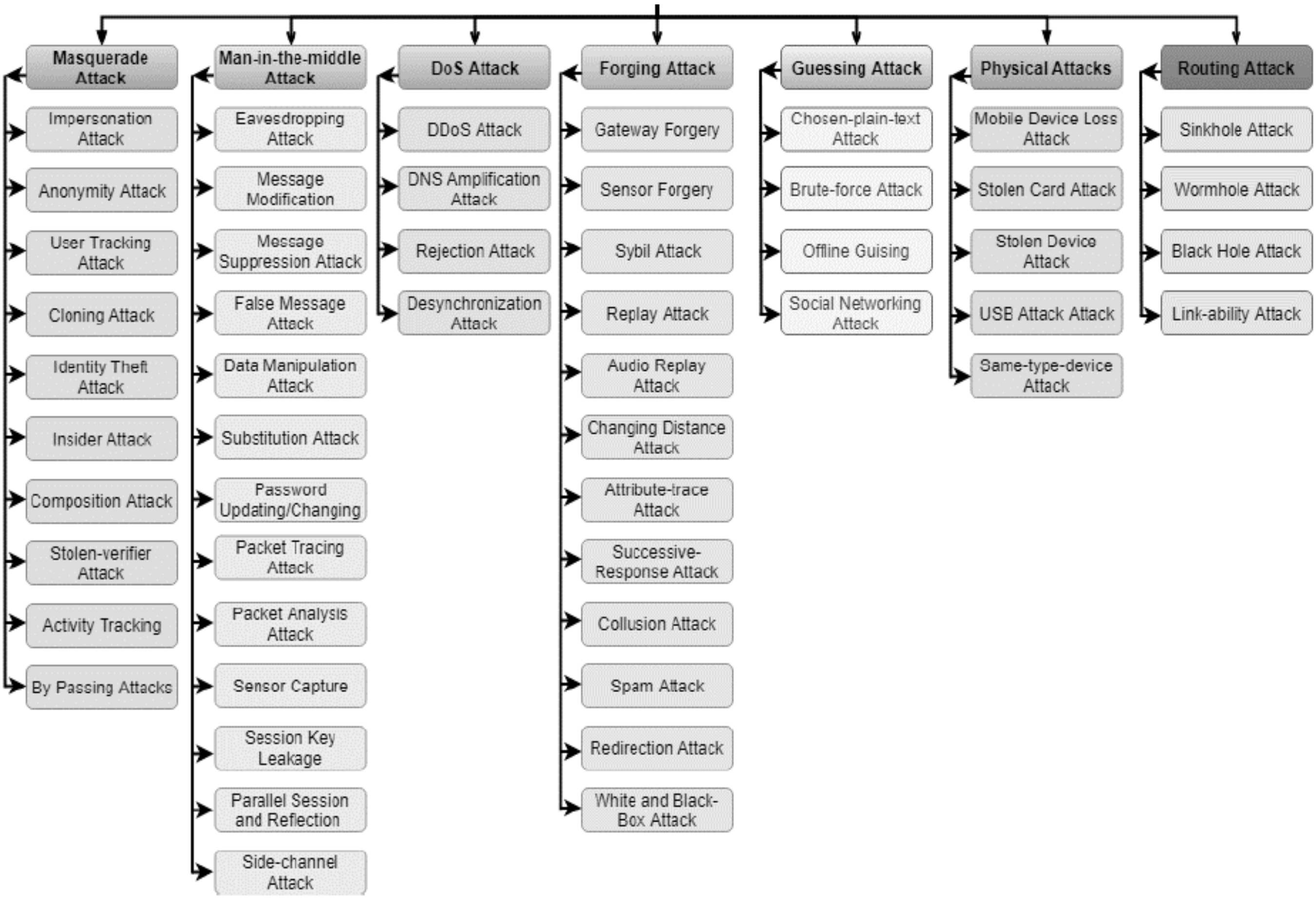

Fig. 4 Taxonomy of attacks on authentication.

uses them to request money from legitimate users' friends and relatives or perform fraudulent transactions. This occurs when the attacker obtains the authorized user's credentials through social engineering techniques and uses them to swap the SIM card. Furthermore, the adversary can also use fake documents to register the SIM cards of legitimate users and have full access to the victims' mobile money accounts [18].

Spoofing attacks: This attack happens when the adversary assumes the role of a mobile system administrator and has full access to the system [19]. This is typical since most mobile money systems and applications have lax security, enabling hackers to compromise them [20].

Social engineering attack: In order to obtain control over the victim's mobile money account, this is the act of manipulating someone to divulge private information, such as a mobile money PIN. Mobile money networks employ PINs to secure mobile money accounts, making them prone to various security risks, such as assaults using social engineering [14]. Attackers use social engineering techniques to circumvent mobile money's 2FA scheme, compromise user accounts, and avoid fraud detection technologies.

Phishing attack: This is a deceitful attempt by adversaries to obtain confidential information such as mobile money PINs from mobile money users and agents by impersonating employees of MMSP in electronic communication [15]. They have further expanded the definition to "A type of mobile money crime occurs when fraudsters impersonate employees of a Mobile Money Service Provider (MMSP) by calling or sending SMS messages to users and agents, asking them to disclose their data, including PINs, for an alleged update" (p. 18). Phishing starts when an adversary intercepts the network traffic between the mobile money user or agent and the mobile money application server and then uses a fraudulent call or message to lure the victim into revealing their credentials. The message is created to look as if it comes from the MMSP. Then, the victim is persuaded to provide the mobile money PIN to the fraudster.

Trojan horse attacks: A Trojan horse is malicious software that, once installed on the phone, either steals sensitive information and sends it to the attacker or creates a backdoor to access the phone. It uses a Trojan horse program employed by hackers and adversaries to compromise the authentication system. Mobile money users and agents are deceived through social engineering to download and run Trojan malware on their phones. Once activated, Trojans can enable hackers to spy on mobile money users and agents, steal their mobile money PINs, and gain backdoor access to their mobile money accounts [21]. Moreover, adversaries can install malware that gives them the exclusive right to redirect users to their network [18].

C. Limitations & Comparison between existing Authentication Mechanisms

In compliance with the NIST 800-63B standard and the levels of authentication offered (NIST, 2020), we have emphasized the potential for developing and executing a hybrid authentication solution utilizing current techniques contingent upon the systems' operational needs. A crucial prerequisite, as stated in the standard below, is a cryptographically secure communication channel between the user and the service provider to help preserve the privacy of the user credentials used for authentication and the re-authentication process, which needs to be carried out regularly, irrespective of the user's activities.

Limitations are addressed in order to provide a more nuanced understanding of the security techniques, demonstrating that although they have many advantages, they also present certain difficulties.

Processing expenses, for these Significant computational resources are needed for several authentication techniques, most notably biometric verification and multi-factor authentication. Biometric data, such as fingerprints or facial recognition, needs to be processed fast and securely. This can lead to increased latency and resource demands, especially in situations with limited resources like Internet of Things (IoT) devices or large-scale networks. For an example, adding facial recognition technology into the current security framework could cause delays that negatively impact the user experience, especially in busy places like airports or big businesses.

Privacy Issues are a major worry, especially when using biometric identification. Biometric information, like fingerprints or facial scans, cannot be reset or altered, in contrast to passwords. The user's data cannot be changed in the event that a biometric database is breached, posing lifetime privacy implications. This gives rise to worries about data misuse, especially in areas where data privacy laws are less strict.

Upon closer inspection of TABLE II, it becomes evident that the hybrid authentication methods, which align with the highest level of protection, AAL3 (Authenticator Assurance Level 3), are among the most resilient authentication factors that enhance security strength. From these protection levels, we can ensure the security level that suits the appropriate authentication method. These techniques are primarily employed in settings where stringent controls over physical and logical access are necessary, such as military and governmental institutions where maintaining information availability, secrecy, and integrity is critical.

Below, TABLE III compares and discusses the benefits and drawbacks of eleven (11) distinct authentication method combinations, including the traditional method. The key factors to compare were cost, accuracy, flexibility, and security performance.

Scalability Issues in Systems for multi-factor and biometric authentication provide robust security, but scalability is frequently an issue. For instance, it can be costly and logistically difficult to manage and maintain several authentication elements (such as physical tokens, biometrics, etc.) in large businesses with thousands of users.

Accessibility and User Experience in Certain techniques, such as dynamic passwords or biometric authentication, may be difficult for consumers to utilize. For instance, customers may perceive biometric systems as untrustworthy if the environment or hardware (such as fingerprint scanners) malfunctions, and OTPs transmitted by SMS are susceptible to SIM-swapping attacks.

As per below TABLE III we have concluded with the given points and factors. From that, Traditional PIN systems are cost-effective but offer low performance and flexibility, making them suitable for less critical applications. Their high accuracy does not compensate for their vulnerability to various types of attacks PIN and Fingerprint: This system balances cost and security more accurately than a PIN alone. However, it lacks flexibility and can still be vulnerable if one of the factors is compromised. Method 3 is more secure than a PIN alone but suffers from issues related to accuracy and performance, especially in challenging environments.

PIN and Iris are highly secure and accurate but have a high cost and low flexibility. They are suitable for high-security environments where accuracy and performance are paramount. Face Detection and OTP methods provide a good balance of security and accuracy but at a medium cost. It is less flexible and may be cumbersome for some users.

Method 6 is versatile and offers good security at a reasonable cost. The ability to switch between OTP and biometric methods adds valuable flexibility. Method 7 offers high security and accuracy but is expensive and limited in flexibility. It is well-suited for environments where maximum security is required. PIN and Face Image offer moderate security but are limited in accuracy and flexibility. They could be better for critical applications where high reliability is required. Method 9 is more expensive and complex. It offers moderate security and accuracy with the added benefit of location-based authentication. However, it needs more flexibility and is costly to implement. PIN, Fingerprint, and OTP are highly secure and accurate, making them suitable for environments requiring maximum security. The cost is moderate, but the need for more flexibility may be a downside for some users. PIN and Fingerprint or S-code and OTP are the most secure and flexible options. They provide multiple layers of authentication at a moderate cost and are ideal for high-security environments where user flexibility is also a priority.

D. Future Prospects

Authenticity is more important now than it has ever been. In the digital age, most users will supplement traditional passwords with biometrics regarding authorization and system security. While worries about privacy, security, usability, and accuracy remain, MFA has developed into a system that guarantees the security and usability that modern consumers require while gaining access to sensitive data. Biometrics are unquestionably one of the most essential elements that will enable MFA in the future. This feature is frequently seen as an addition to more conventional authentication methods like PINs, smart cards, and passwords rather than a stand-alone solution. Combining two or more authentication methods is anticipated to increase security when user verification is performed. The synergistic biometric systems that provide much-enhanced user experience and MFA system throughput, which would be

TABLE II

OVERVIEW OF AUTHENTICATION METHODS RELATED TO ASSURANCE LEVEL [22]

Authentication Method	**Level of Access According to NIST 800-63B**	**Attack Vectors**	**Level of Protection**
Password	AAL1	Man-in-the-middle, Phishing, Dictionary attack, Theft of credential access, Replay attack, social engineering	Low
Pattern-based authentication	AAL1	Man-in-the-middle, Phishing, Social engineering	Low
Token OTP	AAL1	Man-in-the-Middle	Low
FIDO security key	AAL2	Cryptographic attacks, Compromising cryptographic keys	Medium
Cryptographic algorithms/PKI certificates	AAL2	Cryptographic attacks, Compromising cryptographic keys	Medium
Pattern-based authentication + password	AAL2	Man-in-the-middle, Denial of Services, Malware, SQL Injection, Social engineering	Medium
OTP authentication + biometric methods	AAL2	Man-in-the-middle, Brute force attacks, Compromising cryptographic keys	Medium
FIDO security key + biometric methods	AAL3	Cryptographic attacks, Compromising cryptographic keys	High
OTP hardware authentication + password	AAL3	Cryptographic attacks, APT - Advanced Persistent Threat	High
Cryptographic algorithm + password	AAL3	Cryptographic attacks	High
OTP authentication + cryptographic algorithm	AAL3	Cryptographic attacks	High

AAL - Authenticator Assurance Level

TABLE III

COMPARISON OF SECURITY SYSTEMS [23]

No.	Security System	Performance	Accuracy	Cost	Flexibility	Total Score
1	PIN (Classical Method)	VL (0)	VH (8)	VL (5)	N (1)	14
2	PIN and Fingerprint	L (3)	H (6)	L (4)	N (1)	14
3	PIN and Face Detection	L (3)	M (3)	M (3)	N (1)	10
4	PIN and Iris - Retina	H (9)	VH (8)	H (2)	N (1)	20
5	Face Detection and OTP	M (6)	H (6)	M (3)	N (1)	16
6	PIN and OTP or Biometric (Fingerprint)	M (6)	H (6)	M (3)	Y (5)	20
7	Palm Vein and UIN	H (9)	H (6)	H (2)	N (1)	18
8	PIN and Face Image	M (6)	L (0)	M (3)	N (1)	10
9	Sensors with GPS with another method (PIN)	M (6)	M (3)	VH (1)	N (1)	11
10	PIN, Fingerprint and OTP	VH (12)	H (6)	M (3)	N (1)	22
11	PIN and Fingerprint or S-code and OTP	VH (12)	H (6)	M (3)	Y (5)	26

advantageous for numerous applications, are the foundation of the anticipated evolution towards MFA. Refer to Fig. 5. These systems will combine ownership, biometrics, and knowledge intelligently. Considering the MFA model for future trends, we have suggested preparing a security device for our node for efficiency, flexibility, and effectiveness. We can use other factors, such as knowledge and ownership, to prove that the node uses the MFA model. We can build a mobile application with built-in biometric security authentication and look for other authentication factors for the security device.

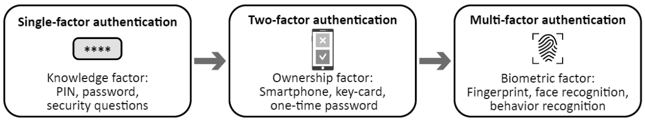
Single-factor authentication
****
Knowledge factor: PIN, password, security questions
Two-factor authentication
Ownership factor: Smartphone, key-card, one-time password
Multi-factor authentication
Biometric factor: Fingerprint, face recognition, behavior recognition

Fig. 5. Evolution of authentication methods from SFA to MFA

Regarding Enhancing Convenient and Privacy-Maintaining Authentication Techniques, Future research can concentrate on creating thin, privacy-preserving authentication techniques that can be successfully implemented in resource-constrained situations, like IoT networks or mobile devices, in light of the restrictions that have been discovered. For instance, combining AI and machine learning algorithms can maximize resource utilization while assisting in the real-time prediction and mitigation of security issues. AI may also be utilized to improve biometric systems by enhancing matching algorithm speed and accuracy without adding significant computing costs.

Combining Blockchain with Decentralized, Secure Authentication has the incorporation of blockchain technology into authentication systems is a potentially fruitful future avenue. In order to handle user identities securely and transparently without depending on a central authority, blockchain technology can offer decentralized, tamper-proof verification processes. By doing this, privacy issues can be resolved and confidence in systems that demand user authentication across many platforms or organizations can be increased.

IV. Conclusion

Despite being the cornerstone of network security, traditional methods like static passwords and basic handshake protocols are becoming less effective against sophisticated cyber threats like Man-in-the-Middle (MitM) and replay attacks. Emerging authentication mechanisms like dynamic password systems, biometric verification, and multi-factor authentication offer promising solutions. However, they also come with challenges regarding implementation complexity, computational overhead, and user privacy. This literature review has looked at the state of security authentication methods for networked access nodes, with a particular focus on wireless technologies. To improve the resilience of authentication systems, the assessment highlights the need for a multi-layered security strategy that combines conventional and cutting-edge methods. Only some techniques can handle every security issue in contemporary networked environments.

Consequently, it is advised to use a hybrid strategy (Multi-factor Authentication and secured device) that uses the advantages of many authentication techniques. The evaluation also finds several vital gaps in the literature, mainly in real-time authentication procedures, user-centric design, and the incorporation of cutting-edge technologies like blockchain and artificial intelligence into authentication frameworks. Future research should concentrate on filling these gaps by creating more effective, scalable, and user-friendly authentication solutions that are simple to integrate into current network architectures. In summary, even though networked access node security has improved significantly, continued research and innovation are essential to staying abreast of the changing threat scenario. This analysis lays the groundwork for further research into creating more robust authentication techniques, ultimately leading to more reliable and safe network environments.

References

[1] E. Sithirasenan, "An EAP Framework for Unified Authentication in Wireless Networks," 2011, doi: 10.1109/TrustCom.2011.50.

[2] M. T. I. Year, M. C. Reddy, and C. S. Vorugunti, "Notes on ' An Effective ECC based User Access Control Scheme with Attribute based Encryption for WSN '".

[3] S. Boonkrong, *Authentication and access control: Practical cryptography methods and tools*. 2020. doi: 10.1007/978-1-4842-6570-3.

[4] A. M. Gamundani, A. Phillips, and H. N. Muyingi, "An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications," *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, pp. 50–57, 2018, doi: 10.1109/Cybermatics_2018.2018.00043.

[5] P. Patel and S. Upadhyay, "A Brief Survey on Video Authentication," *Int J Sci Res*, vol. 2, no. 2, pp. 61–67, 2012, doi: 10.15373/22778179/feb2013/24.

[6] Y. Yu, J. He, N. Zhu, F. Cai, and M. S. Pathan, "A new method for identity authentication using mobile terminals," *Procedia Comput Sci*, vol. 131, pp. 771–778, 2018, doi: 10.1016/j.procs.2018.04.323.

[7] Z. A. Zukarnain, A. Muneer, and M. K. Ab Aziz, "Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges," *Symmetry (Basel)*, vol. 14, no. 4, 2022, doi: 10.3390/sym14040821.

[8] A. Sarkar and B. K. Singh, "A review on performance,security and various biometric template protection schemes for biometric authentication systems," *Multimed Tools Appl*, vol. 79, no. 37–38, pp. 27721–27776, 2020, doi: 10.1007/s11042-020-09197-7.

[9] K. Reese *et al.*, "A Usability Study of Five Two-Factor Authentication Methods This paper is included in the Proceedings of the," pp. 357–370, 2019.

[10] M. Nerini, E. Favarelli, and M. Chiani, "Augmented PIN Authentication through Behavioral Biometrics," *Sensors*, vol. 22, no. 13, pp. 1–15, 2022, doi: 10.3390/s22134857.

[11] M. O-Genseleke, O. Ebenezer, and C. Chigozie-Okwum, "Implementation of Multifactor based Authentication Scheme for Enhanced ATM Security," *Int J Comput Appl*, vol. 181, no. 1, pp. 48–51, 2018, doi: 10.5120/ijca2018917400.

[12] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, pp. 1–31, 2018, doi: 10.3390/cryptography2010001.

[13] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.

[14] G. Ali, M. A. Dida, and A. E. Sam, "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures," *Future Internet*, vol. 12, no. 10, pp. 1–27, 2020, doi: 10.3390/fi12100160.

[15] G. Ali, M. A. Dida, and A. E. Sam, "Evaluation of key security issues associated with mobile money systems in Uganda," *Information (Switzerland)*, vol. 11, no. 6, pp. 1–24, 2020, doi: 10.3390/info11060309.

[16] M. W. Buku and R. Mazer, "Fraud in Mobile Financial Services," *Cgap*, pp. 1–4, 2017, [Online]. Available: http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf

[17] G. Raphael, "Risks and Barriers Associated with Mobile Money Transactions in Tanzania," *Business Management and Strategy*, vol. 7, no. 2, p. 121, 2016, doi: 10.5296/bms.v7i2.10069.

[18] M. Bosamia and D. Patel, "Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 1, pp. 810–817, 2019, doi: 10.26438/ijcse/v7i1.810817.

[19] I. Akomea-Frimpong, C. Andoh, A. Akomea-Frimpong, and Y. Dwomoh-Okudzeto, "Control of fraud on mobile money services in Ghana: an exploratory study," *Journal of Money Laundering Control*, vol. 22, no. 2, pp. 300–317, 2019, doi: 10.1108/JMLC-03-2018-0023.

[20] B. Reaves *et al.*, "Mo(bile) money, mo(bile) problems: Analysis of branchless banking applications," *ACM Transactions on Privacy and Security*, vol. 20, no. 3, 2017, doi: 10.1145/3092368.

[21] S. Singha, R. Ressel, D. Velotto, and S. Lehner, "A Combination of Traditional and Polarimetric Features for Oil Spill Detection Using TerraSAR-X," *IEEE J Sel Top Appl Earth Obs Remote Sens*, vol. 9, no. 11, pp. 4979–4990, 2016, doi: 10.1109/JSTARS.2016.2559946.

[22] G. Crihan, M. Craciun, and L. Dumitriu, "Hybrid Methods of Authentication in Network Security," *The Annals of "Dunarea de Jos" University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics*, vol. 45, no. 1, p. 7, 2023, doi: 10.35219/eeaci.2022.1.02.

[23] M. J. A. Sabani, and U. M. Rishan, "Effectiveness of Atm Security Mechanisms: a Review Analysis," *Proceedings of 9th International Symposium*, no. July, pp. 234–243, 2020.