Authentication Techniques in 5G Network Slicing Security: A Survey

Essam A. Abduh (*,1)
Belal A. Al-Fuhaidi [2]
Fahd A. Alqasemi [1]

[1] Department of Information Technology, Faculty of Computing and Information Technology, University of Science and Technology, Ibb, Yemen

[2] Department of Computer Science, Faculty of Computing and Information Technology, University of Science and Technology, Sana'a, Yemen

* Corresponding author: e.aamb2010@gmail.com

https://doi.org/10.59222/ustjet.2.2.2

Authentication Techniques in 5G Network Slicing Security: A Survey

Abstract:

Emerging network slicing technology is a key feature of 5G cellular networks. Network slice and cloud computing provide promising solutions in 5G architecture. Network Slicing Security (NSS) is also important in 5G research. The emerging environment is a fertile breeding ground for the attacker. This study discusses authentication techniques in fifth-generation networks, as the authentication process is the first wall of defense against various network attacks. Meanwhile, techniques and algorithms are important in achieving confidentiality, integrity, and availability while maintaining speed and accuracy. The diversity and multiplicity of devices, in addition to the movement between slices and operators, make the authentication process extremely important. This article presents and explains the main issues related to network segment threats and attacks, highlighting the authentication techniques used in NS. The authentication process mainly focuses on the use of encryption and digital signature technology, either implicitly within the devices or directly when connecting to the network.

Keywords: 5th generation networks (5G), network slicing (NS), NS security, data encryption, hashing functions, convolutional neural network.

https://doi.org/10.59222/ustjet.2.2.2

تقنيات المصادقة في أمان شرائح شبكة الجيل الخامس: دراسة مسحية

الملخص:

تعد تقنية شرائح الشـبكة الناشئة سمة أساسية لشبكات الجيل الخامس الخلوية. توفر شرائح الشـبكة والحوسبة السـحابية حلولاً واعدةً في بنية الجيل الخامس. كما أن أمان شرائح الشبكة (NSS) مهم في أبحاث الجيل الخامس. البيئة الناشئة هي أرض خصبة لتكاثر المهاجمين. تناقش هذه الدراسـة تقنيات المصادقة في شبكات الجيل الخامس، حيث تعد عملية المصادقة هي الجدار الدفاعي الأول ضد هجمات الشبكة المختلفة. وفي الوقت نفسه، تعد التقنيات والخوارزميات مهمة في تحقيق السرية والنزاهة والتوافر مع الحفاظ على السرعة والدقة. إن تنوع وتعدد الأجهزة، بالإضافة إلى الحركة بين الشـرائح والمشـغلين، يجعل عملية المصادقة مهمة للغاية. تقدم هذه المقالة وتشرح القضايا الرئيسية المتعلقة بتهديدات وهجمات شريحة الشبكة، مع تسليط الضوء على تقنيات المصادقة المسـتخدمة في NS. تركز عملية المصادقة بشـكل اساسـي على استخدم تقنية التشفير والتوقيع الرقمي سواء بشكل ضمني ضمن الاجهزة او بشكل مباشر عند الاتصال بالشبكة.

الكلمات المفتاحية: شـبكات الجيل الخامس (5G)، شـرائح الشـبكة (NS)، أمان شرائح الشبكة؛ تشفير البيانات، وظائف التجزئة، الشبكة العصبية التلافيفية.

1. Introduction

5G is an advanced generation of wireless technologies that is also revolutionizing network service architecture. Network slicing is one of the key technologies that distinguishes 5G networks from 4G networks, where the slice itself forms a logical private network. 5G wireless networks support billions of devices that will be connected to the Internet by the end of 2025, based on the expectation that more than 50 billion devices will use cellular network services [1]. It would increase a large amount of data traffic.

Attackers and impersonators take advantage of loopholes and vulnerabilities in any system to illegally access data and information. They have many tools and means to make the victim fall into their nets. They even develop and take care of it continuously. The diversity of IoT devices, the number of users, as well as the amount of data circulating within the network, pose an opportunity for hackers and impersonators to illegally access data and information [2].

The global annual cost of cybercrime is expected to reach US$9.5 trillion in 2024. Compounding this is the rising cost of damage from cybercrime, which is expected to reach US$10.5 trillion by 2025 [3]. In 2023, 81% of organizations were exposed to ransomware attacks, and 48% of them paid the ransom [4].

The 5G network and network slice support for many new trends, IoT, and smart cities resulting in the re-authentication process constitutes another opportunity for the attacker to enter the network. All of this causes delays in the authentication process due to the large amount of movement that occurs when traveling from one place to another. Most of these mentioned factors are achieved in the 5G network, especially in network slicing. Because the authentication process is the first opportunity for an attacker to access data [5].

This study sheds light on authentication techniques related to slicing 5G networks. By presenting an introduction to the importance and contributions of fifth-generation networks. The role of network slicing in supporting many cases and applications. Attacks and threats related to NS security. At the same time, it presents the most important studies related to authentication, as well as the techniques used in NS.

https://doi.org/10.59222/ustjet.2.2.2

The remainder of this paper's organization begins with the background of NS in Section II, the main attacks of NS in Section III, and NS authentication and techniques in Sections IV and V, in connection. The last, section six, is a conclusion of the results of this study.

2. Network Slicing

Network Slicing (NS) is a key concept in 5G networks that allows the creation of multiple virtual networks on a shared physical infrastructure. It enables the customization and optimization of network resources to meet the specific requirements of different use cases, applications, or industries [6].

In NS, the 5G infrastructure has been divided into independent and logically isolated virtual networks, referred to as NS. Each NS is dedicated to a particular use case or application; it is tailored to provide the required performance, capacity, latency, security, and Quality of service (QoS) characteristics [7]. The distinction between a standard network and a network sliced is illustrated in Figure 1.

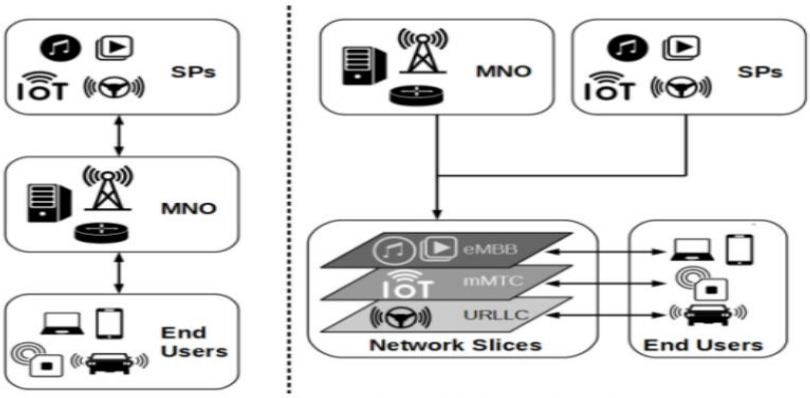

Figure 1: Sliced Network Vs Unsliced Network [8]

Intra-network slicing refers to moving between different slices within a single network operator's infrastructure. Which makes the user need to re-authenticate with the slice to ensure that the resource is used by authorized parties [9].

Inter-network slicing refers to cooperation and coordination between multiple network operators to provide comprehensive services across different network domains. To ensure services progress smoothly across diverse environments. This makes the user need to re-authenticate when moving from one operator to another [10].

Authentication in 5G NS refers to the process of verifying the identities of entities involved in NS and ensuring secure access to the network resources and services within a slice. It plays a crucial role in establishing trust, preventing unauthorized access, and maintaining the integrity and confidentiality of the NS. There are many key aspects of authentication in 5G NS such as subscriber authentication, device authentication, mutual authentication, authentication protocols, key management, access control, and continuous authentication.

The authentication process varies depending on the NS, the services they provide, and the devices that support them, NS supports many services and technologies.

3. 5G Network Slice Security

NS in 5G networks introduces new attack surfaces and potential vulnerabilities that adversaries may target. This shows that the secure authentication process is a barrier against many attacks. Here are some examples of attacks that might directed against NS:

A. Slice Hijacking

Adversaries may attempt to hijack or take control of an NS, gaining unauthorized control over its resources and operations. This can enable them to manipulate or disrupt the services provided by the slice or launch further attacks within the compromised slice [1] [10].

B. Cross-Slice Interference

Attacks can be directed towards causing interference or disruption between different network slices. This interference can impact the performance, reliability, or QoS of multiple slices, affecting the services and applications they support [11] [12].

C. Unauthorized Slice Creation or Modification

Attackers may try to create or modify NS without proper authorization. This can lead to unauthorized access to resources, misconfiguration of slice parameters, or the introduction of malicious slices that can compromise the overall network infrastructure [13] [14].

D. Slice Denial of Service (SDoS)

Adversaries may launch denial-of-service attacks specifically targeting NS. By overwhelming a slice with excessive traffic or requests, they can disrupt the

https://doi.org/10.59222/ustjet.2.2.2

services provided by that slice, impacting the applications and users relying on it [15][16].

E. Slice Traffic Interception or Manipulation

Attackers may attempt to intercept or manipulate the traffic flowing within an NS. This can lead to the unauthorized access, modification, or theft of sensitive data, compromising the integrity and confidentiality of the slice's operations.

F. Virtualized Infrastructure Attacks

NS relies on virtualized infrastructure components, such as virtual machines (VM), SDN, and virtual network functions (VNF). Adversaries may exploit vulnerabilities in these virtualized components to gain unauthorized access, control, or disrupt the network slices [17]. To mitigate these attacks, network operators and service providers need to implement robust security measures and best practices. This includes strong access controls, encryption, traffic monitoring, intrusion detection and prevention systems, security audits, and regular patching and updates of the network infrastructure. Additionally, strong authentication and authorization mechanisms should be enforced to ensure proper access to network slices, and security monitoring should be in place to detect and respond to potential attacks promptly [18].

4. Authentication in 5G Network Slicing

Authentication in 5G NS refers to the process of verifying the identities of entities involved in NS and ensuring secure access to the network resources and services within a slice. It plays a crucial role in establishing trust, preventing unauthorized access, and maintaining the integrity and confidentiality of the NS. There are many key aspects of authentication in 5G NS such as subscriber authentication, device authentication, mutual authentication, authentication protocols, key management, access control, and continuous authentication. Subscriber authentication ensures that only authorized individuals or devices can connect to a specific slice. This authentication is typically performed using credentials, such as usernames, passwords, or digital certificates, which are validated by the network infrastructure.

Third-party service providers can rent slices within the 5G network with the use of NS. Additionally, Service Level Agreements (SLA) about metrics like service quality and data bandwidth could be made with operators. The main security concern, according to [19]. How to manage access authentication

and approval for a specific NS is described in [15]. In the context of the Internet of Things, [20] presented a service-oriented authentication system enabling network-slicing IoT.

During the registration process, this framework enables users to obtain anonymous authentication tickets that have been approved by operators and IoT servers (ISV). These anonymous authentication tickets could be used for ISV authentication when users make service requests. Although a network-slicing authentication system was proposed in this study, the inter-slice handover was not taken into account. The authentication phase had a substantial overhead because it required users to send tickets to the ISV for approval during the authentication phase and because this framework adopted the bilinear pairing cryptology primitive. For instance, processing handover authentication on the user side would cost 332.544 milliseconds, which did not meet the requirement for a real-time service.

The ticket in [21] was not a feature that was available to all users because only an abstract ISV authentication server was created for this model, which failed to account for the adoption of multiple ISV servers in the configuration of network segments. As a result, a separate mechanism was needed to complete inter-slice handover authentication. Additionally, a novel re-encrypted strategy based on agencies was suggested by [22]. to achieve secure collaboration among Network Slice Components [15][18]. (NSCs). This method offers anonymous services for NSC groups under the Service Provider by utilizing bilinear properties on the elliptic curve (SP).

According to the protocols proposed by [15][23]. (2015), NSCs working under different SPs are unable to distinguish between the identities of SPs, which may lead to slice isolation. [24]. [25] proposed an authentication mechanism called 5G-Slice Specific Authentication and Access Control (5G-SSAAC), which could lighten the load on the core network by entrusting the third-party slice providers with user identity authentication and access control. [23] only raised a protocol framework without presenting the actual realization of the protocol. Based on the work of [26]. [25] they [21] developed a new network function for the 5G Radio Access Network (RAN).

Specifically, they designed the protocols for users to link third-party slices, forcing the third-party slice providers to choose the appropriate Authentication and Access Control (AAC) for their security requirements.

https://doi.org/10.59222/ustjet.2.2.2

When developing the batch authentication approaches, [27] and [28]. [27] and [29] concentrated on power injection in the 5G smart grid slice. The research by [29] and [28] used hash-then-homomorphic technology and non-certificate aggregate signature technology, respectively. A supplement was developed by [15]. to aid peer-to-peer users in protecting their anonymity. [28] proposed a grouping anonymous mutual authentication method of anti-topological learning attacks during the slice's formulation stage. Moreover, a group anonymous one-way authentication method is proposed to protect users' service access behavior. Even though all of the aforementioned authentication strategies were based on network slices, they neglected to account for the users' requirement for speedy verification during inter-slice handover.

Therefore, the prior effort falls short of the requirement for quick inter-slice handover authentication. Table 1. shows: related studies present the techniques, objectives, and results that have been reached, which show continuous attempts to improve the authentication process by reducing the communication overhead process, which depends mainly on the tools used in the 5G network.

Table 1: Authentication in 5G Slices

Study	Problem	Evaluation	Shortcoming	Finding
[23]	Increasing the load of the connectivity in Authentication and Access Control (AAC)	Open Air Interface (OAI)	The opportunity to overcome the security shortcomings in their AAC mechanisms	Decreasing the load of the connectivity provider's CN
[24]	Increasing the load of the connectivity in AAC	OAI	The opportunity to overcome the security shortcomings in their AAC mechanisms	Reduces the AAC signaling load on
[30]	Privacy in Inter-Slice Handover Authentication	Compare with ES3 A, CPAL, and LCCH schemes	This solution has the largest communication overhead. This is because ring signatures have been introduced in the registration phase.	There has been a 97.94 percent decrease in inter-slice transfer delay.

Table 1: Continued

Study	Problem	Evaluation	Shortcoming	Finding
[21]	the authentication is decentralized to the edge clouds to achieve low latency	Compared with [20].	It is immune to one attack, replay attacks	Enhance the computation cost and the latency
[19]	A comprehensive survey on the security of 5G V2X services	---	Access authentication and authorization cached data confidentiality when the edge nodes	A brief overview of key challenges in securing 5G V2X.
[28]	Security of transmitted information and users' privacy preservation	Comper with another scheme	Suitable for practical application in power injection system	Goals of batch verification, anonymity, nonrepudiation, and conditional privacy preservation. reduced storage overhead
[18]	Ensuring Availability legitimate components isolation	Compare to the CBAKE protocol		Has 9.52% less computation overhead and 13.64% less bandwidth overhead preventing targeted DDoS
[20]	Security and privacy (elusive)	Simulations	ES3A is less efficient than YHWD in communication overhead on service authentication and lowest in communication bandwidth on the credentials and authentication.	Demonstrated security and privacy preservation and efficiency. build secure data channels for the access of the service data
[31]	Security issues among the heterogeneous systems	Compare with WLZ, LZT, LHJ, and ZZW	WLZ achieves the lowest computation cost because there is no scalar multiplication but only a few bilinear pairings	Schemes achieve greater efficiency and security. more efficient on the computational overhead

https://doi.org/10.59222/ustjet.2.2.2

Table 1: Continued

Study	Problem	Evaluation	Shortcoming	Finding
[32]	Security and privacy issues in autonomous vehicle networks AVNs			Security and privacy issues in autonomous vehicle networks AVNs
[2]	Security and privacy	---	--	Enhances readers' understanding of specific 5G application security risks and solutions.
[33]	Mutually authenticate and ensure the data confidentiality and integrity	Compare authentication message, session key, and identity		Perfectly withstand replay attacks. So our protocol applies to the WBAN and mobile networks
[34]	Despite growing interest in ECG authentication	Compare with 48 patients in the MIT-BIH database and 90 people in the ECG ID database		Achieved 100% accuracy when evaluated with 48 patients in the MIT-BIH database and 90 people in the ECG ID database.

It appears from Table 2: Most studies deal with the process of preparation, registration, and authentication, in addition to the process of transferring within Intra-slice or between Inter-slice service operators.

Table 2: Basic Authentication Operations in Network Slice

No	References	Initialize or Setup	Registration	Authentication	Handover	Inter-slice	Intra-slice
1.	[23]	√	√	√	X	X	X
2.	[24]	√	√	√	X	X	X
3.	[30]	√	√	√	√	√	√
4.	[19]	√	√	√	X	X	X
5.	[28]	√	√	√	X	X	X
6.	[18]	√	X	√	X	√	X
7.	[20]	√	√	√	X	X	X
8.	[33]	√	√	√	X	X	X

Table 2: Continued

No	References	Initialize or Setup	Registration	Authentication	Handover	Inter-slice	Intra-slice
9.	[34]	√	√	√	X	X	X
10.	[35]	√	√	X	√	X	√
11.	[15]	√	√	√	√	X	X
12.	[36]	√	√	√	√	X	X
13.	[37]	√	√	√	√	√	√

5. NS Authentication Techniques

This section discusses some important techniques that are utilized for authentication in network slicing security.

A. Blockchain

Blockchain is a technique for storing data that makes it difficult or impossible for the system to be altered, hacked, or otherwise interfered with. A distributed ledger known as a blockchain copies and distributes transactions among the network of computers involved in the blockchain. In an increasingly digital environment, blockchain technology has several benefits: i) Very Secure ii) A decentralized system iii) Automation capability blockchain, also known as distributed ledger technology (DLT), uses a decentralized network and cryptographic hashing to make the history of any digital asset transparent and unchangeable. Using blockchain technology for 5G authentication procedures an immutable distributed ledger is made possible by blockchain technology. Figure 2 shows a simple structure of Blockchain.

The second version of this technology enables the execution of smart contracts, which are programmable transactions. Between the Serving Network (SN) and Home Network (HN), blockchain for 5G authentication may act as a barrier. By doing this, blockchain can offer a safe conduit for message exchange. Preventing malicious SNs, which can operate as active attackers, from accessing the HN, encourages user anonymity and defends the HN from DoS attacks. Additionally, it offers an auditable, tamper-proof log of the authentication procedures [38][39]. Every transaction in this ledger is validated and protected against fraud by the owner's digital signature, which also serves to authenticate the transaction. As a result, the data in the digital ledger is quite safe. Such remote attestation systems are possible to create using the blockchain as a technology.

https://doi.org/10.59222/ustjet.2.2.2

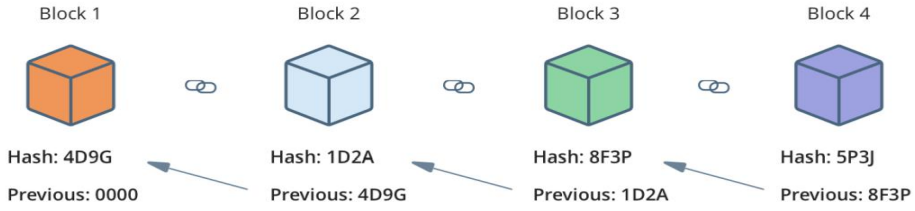

Figure 2: Structure of Blockchain

B. Chameleon Hash

Chameleon Hash is a hash functions that have a trapdoor that enables one to identify arbitrary collisions within the functions' domain, which are known as chameleon-hash functions (CHF), or trapdoor-hash functions for short. On the other hand, as long as the associated trapdoor is unknown, CHF is collision-resistant [40][41]. A CHF is an extended notion of the hash function, with the following properties: (i) for each function exists a pair of hashing/ trapdoor keys, (ii) anyone who has hashing keys can generate the hash function, (iii) the owner of the trapdoor keys can find collisions in the domain of the function. (iv) The function remains collision-resistant for anyone without trapdoor keys [42].

CHF was introduced by Krawczyk and Rabin, Chameleon-hash functions have also proven useful in other areas such as Verifiable image revision [43], Privacy Preservation in E-Governance Systems [40], secure signature and identity-based encryption [44].

When just the hashing keys of the functions are known, chameleon hash functions are collision-resistant. Specifically without being aware of the sensitive information. No one can calculate collisions without knowing the trapdoor keys, even if he can observe collisions for every given hash function. [42] The collision resistance hash function CHAM-HASHR, also known as a trapdoor hash function, has the non-standard property of being collision-resistant for the signer and collision-traceable for the recipient. Trapdoor one-way is a necessary component of chameleon hashing. a public key (also known as a hash key) and private key (also known as a trapdoor key) pair.

C. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a cryptographic approach that utilizes the mathematical properties of elliptic curves to provide secure communication and encryption. It is a form of public-key cryptography, where each participant has a pair of keys: a private key and a corresponding public key. The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), which involves finding the private key given the public key. The underlying mathematics of elliptic curves make this problem computationally infeasible to solve efficiently [45]. One of the main advantages of ECC is its ability to provide the same level of security with smaller key sizes compared to other traditional public key cryptosystems like RSA. This makes ECC more resource-efficient, as smaller keys require less computational power and storage capacity. It is particularly advantageous in constrained environments such as mobile devices and embedded systems [46][47]. ECC is widely used in various applications, including secure communication protocols, digital signatures, key exchange protocols, and secure data transmission.

Many standardized protocols and algorithms, such as those defined by the National Institute of Standards and Technology (NIST), incorporate ECC. While ECC offers significant benefits, it is important to ensure the proper selection of elliptic curves and the implementation of secure protocols to maintain its security [48]. Ongoing research and analysis are necessary to identify any potential vulnerabilities and to keep ECC algorithms secure. In the end, ECC is a powerful cryptographic technique that leverages the mathematical properties of elliptic curves. Its smaller key sizes and resource efficiency make it a popular choice for secure communication and encryption in various applications, providing strong security while conserving computational resources.

Table 3 shows the most important technologies used in the authentication process in network slice, as these technologies affect the devices connected to the network.

https://doi.org/10.59222/ustjet.2.2.2

Table 3: Important Technologies Used in the Authentication Process in Network Slice

Study	Problem	Techniques
[23]	Increasing the load of the connectivity in Authentication and Access Control (AAC)	Actual RAN, with the OAI
[24]	Increasing the load of the connectivity in AAC	Actual RAN, with the OAI
[30]	Privacy in Inter-Slice Handover Authentication	Chameleon hashing, ring signature, and blockchain technologies Simulation framework
[21]	the authentication is decentralized to the edge clouds to achieve low latency	Elliptic curve encryption one-way hashing
[19]	A comprehensive survey on the security of 5G V2X services	--
[28]	Security of transmitted information and users' privacy preservation	Certificateless aggregate signature (CL-AS) algorithm
[18]	Ensuring Availability legitimate components isolation	Proxy re-encryption on elliptic curve
[20]	Security and privacy (elusive)	Hash and encryption /decryption algorithms
[31]	Security issues among the heterogeneous systems	Bilinear Pairings
[32]	Security and privacy issues in autonomous vehicle networks AVNs	Hash-then-homomorphic technique and the Paillier Cryptosystem
[2]	Security and privacy	Present a use case of access control and make conclusions
[33]	Mutually authenticate and ensure the data confidentiality and integrity	Lippold model Simulation
[34]	Despite growing interest in ECG authentication	The convolutional Neural Network (RDSCNN) algorithm was used for the classification

6. Conclusion

The 5G network is a new generation that has many features and services. It is also vulnerable to many threats and attacks of various kinds. One of the services provided by 5G networks is slicing networks into many virtual networks. Network slicing authentication is a very important topic of discussion and explanation regarding promising 5G services and products. This study

has demonstrated the concept of network anatomy, in terms of NS function and NS types. Then the most important security threats and challenges facing this field were explained. Attacks such as chip hijacking and authentication fraud, as well as many others, have been reported.

Next, this survey discussed the most important studies related to authentication and the techniques that have been exploited to avoid some security problems in NS. It highlighted technologies such as Blockchain for secure data management and modern encryption methods. This study aimed to review the most important techniques and tools used in authentication that provide protection and privacy to NS. Which contributes to improving many of the services provided by network slicing.

References

[1] N. Panwar and S. Sharma, "Security and Privacy Aspects in 5G Networks," in *2020 IEEE 19th International Symposium on Network Computing and Applications, NCA 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/NCA51143.2020.9306740

[2] Q. Qiu, S. Liu, S. Xu, and S. Yu, "Study on Security and Privacy in 5G-Enabled Applications," *Wirel. Commun. Mob. Comput.*, vol. 2020, 2020, doi: 10.1155/2020/8856683

[3] Steve Morgan, "Cybercrime To Cost The World 8 Trillion Annually In 2023," *07,Oct*, 2022.

[4] J. FOX, "Top Cybersecurity Statistics for 2024," *cobalt*, 2023.

[5] F. Z. Yousaf et al., "Network Slicing with Flexible Mobility and QoS / QoE Support for 5G Networks," pp. 1–7, 2017.

[6] M. A. Abdel-Malek, K. Akkaya, A. Bhuyan, M. Cebe, and A. S. Ibrahim, "Enabling Second Factor Authentication for Drones in 5G using Network Slicing," *2020 IEEE Globecom Work. GC Wkshps 2020* - Proc., pp. 1–6, 2020, doi: 10.1109/GCWkshps50303.2020.9367441

[7] K. Sevim and T. Tugcu, "Handover with Network Slicing in 5G Networks," in *2021 International Conference on Computer, Information and Telecommunication Systems (CITS)*, IEEE, Nov. 2021, pp. 1–6. doi: 10.1109/CITS52676.2021.9618576

[8] S. Port, U. Case, R. M. Sohaib, O. Onireti, Y. Sambo, and M. A. Imran, "Network Slicing for Beyond 5G Systems : An Overview of the," 2021.

[9] B. Bordel, A. B. Orúe, and D. Sánchez-de-rivera, "An Intra-Slice Security Solution for Emerging 5G Networks Based on Pseudo-Random Number Generators," 2018, doi: 10.1109/ACCESS.2018.2815567

https://doi.org/10.59222/ustjet.2.2.2

[10] M. M. Sajjad, C. J. Bernardos, D. Jayalath, S. Member, Y. Tian, and S. Member, "Inter-Slice Mobility Management in 5G : Motivations , Standard Principles , Challenges and Research Directions," 2022.

[11] Z. Han and J. Liang, "The Analysis of Node Planning and Control Logic Optimization of 5G Wireless Networks under Deep Mapping Learning Algorithms," *IEEE Access*, vol. 7, pp. 156489–156499, 2019, doi: 10.1109/ACCESS.2019.2949631

[12] H. Zhang, N. Liu, X. Chu, K. Long, A. H. Aghvami, and V. C. M. Leung, "Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 138–145, 2017, doi: 10.1109/MCOM.2017.1600940

[13] J. Cáceres and D. Avila-pesantez, "Cybersecurity study in 5G network Slicing Technology : A systematic mapping review," no. October, 2021, doi: 10.1109/ETCM53643.2021.9590742

[14] A. Jain, T. Singh, S. K. Sharma, and V. Prajapati, "Implementing security in iot ecosystem using 5g network slicing and pattern matched intrusion detection system: A simulation study," *Interdiscip. J. Information, Knowledge, Manag.*, vol. 16, pp. 1–38, 2021, doi: 10.28945/4675

[15] V. N. Sathi and C. S. R. Murthy, "Distributed Slice Mobility Attack : A Novel Targeted Attack," vol. 3, no. 1, pp. 5–9, 2021.

[16] A. T. Radar, "On the Rollout of Network Slicing in Carrier Networks : A Technology Radar," pp. 1–52, 2021.

[17] E. Edition, E. Edition, O. Systems, S. Edition, B. D. Communications, and S. Edition, *THE WILLIAM STALLINGS BOOKS ON COMPUTER DATA AND COMPUTER COMMUNICATIONS , EIGHTH EDITION*.

[18] V. N. Sathi, M. Srinivasan, P. K. Thiruvasagam, and S. R. M. Chebiyyam, "A novel protocol for securing network slice component association and slice isolation in 5G networks," *MSWiM 2018 - Proc. 21st ACM Int. Conf. Model. Anal. Simul. Wirel. Mob. Syst.*, pp. 249–253, 2018, doi: 10.1145/3242102.3242135

[19] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G Vehicle-to-Everything Services: Gearing up for Security and Privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, 2020, doi: 10.1109/JPROC.2019.2948302

[20] J. Ni, S. Member, X. Lin, and X. S. Shen, "Efficient and Secure Service-oriented Authentication Supporting Network Slicing for 5G-enabled IoT," vol. 8716, no. c, pp. 1–14, 2018, doi: 10.1109/JSAC.2018.2815418

[21] C. Fan, Y. Shih, J. Huang, and W. Chiu, "Cross-Network-Slice Authentication Scheme for the 5 th Generation Mobile Communication System," vol. 18, no. 1, pp. 701–712, 2021, doi: 10.1109/TNSM.2021.3052208

[22] V. N. Sathi and C. S. R. Murthy, "DSM Attack Resistant Slice Selection in 5G," vol. 2337, no. c, pp. 1–5, 2021, doi: 10.1109/LWC.2021.3070322

[23] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "5G-SSAAC: Slice-specific Authentication and Access Control in 5G," *Proc. 2019 IEEE Conf. Netw. Softwarization Unleashing Power Netw. Softwarization, NetSoft 2019*, pp. 281–285, 2019, doi: 10.1109/NETSOFT.2019.8806667

[24] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 46–61, 2020, doi: 10.1016/j.future.2020.02.014

[25] C. F. Member, J. Huang, M. Zhong, and R. H. Member, "ReHand : Secure Region-based Fast Handover with User Anonymity for Small Cell Networks in Mobile Communications," *IEEE Trans. Inf. Forensics Secur.*, vol. PP, no. c, p. 1, 2019, doi: 10.1109/TIFS.2019.2931076

[26] S. Behrad, "To cite this version : HAL Id : tel-02614232 6OLFH 6SHFLILF $ XWKHQWLFDWLRQ DQG $ FFHVV & RQWURO IRU *," 2020.

[27] S. Zhang, "An Overview of Network Slicing for 5G," *IEEE Wirel. Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019, doi: 10.1109/MWC.2019.1800234

[28] I. A. Kamil and S. O. Ogundoyin, "A big data anonymous batch verification scheme with conditional privacy preservation for power injection over vehicular network and 5G smart grid slice," *Sustain. Energy, Grids Networks*, vol. 20, p. 100260, 2019, doi: 10.1016/j.segan.2019.100260

[29] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *J. Netw. Comput. Appl.*, vol. 122, pp. 50–60, 2018, doi: 10.1016/j.jnca.2018.07.017

[30] Z. Ren, X. Li, Q. Jiang, Q. Cheng, and J. Ma, "Fast and Universal Inter-Slice Handover Authentication with Privacy Protection in 5G Network," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/6694058

[31] J. Liu, L. Zhang, R. Sun, X. Du, and M. Guizani, "Mutual Heterogeneous Signcryption Schemes for 5G Network Slicings," *IEEE Access*, vol. 6, pp. 7854–7863, 2018, doi: 10.1109/ACCESS.2018.2797102

[32] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *J. Netw. Comput. Appl.*, vol. 122, pp. 50–60, 2018, doi: 10.1016/j.jnca.2018.07.017

[33] Z. Zhang, Y. Sun, W. Zhang, Y. Wu, and Z. Qin, "A strongly secure PF-CL-AKA protocol with two-way ID-based authentication in advance for smart IoT devices," *J. Phys. Conf. Ser.*, vol. 1812, no. 1, 2021, doi: 10.1088/1742-6596/1812/1/012038

https://doi.org/10.59222/ustjet.2.2.2

[34] E. Ihsanto, K. Ramli, D. Sudiana, and T. S. Gunawan, "Fast and accurate algorithm for ECG authentication using residual depthwise separable convolutional neural networks," *Appl. Sci.*, vol. 10, no. 9, 2020, doi: 10.3390/app10093304

[35] F. S. D. Silva, L. M. Schneider, D. Rosário, and A. V Neto, "Network Slicing Mobility Aware Control to Assist Handover Decisions on e-Health 5G Use Cases," no. June, 2022, doi: 10.1109/IWCMC55113.2022.9825010

[36] F. Meneses, R. Silva, D. Corujo, A. Neto, and R. L. Aguiar, "Dynamic network slice resources reconfiguration in heterogeneous mobility environments," no. February, pp. 1–6, 2019, doi: 10.1002/itl2.107

[37] Y. Zhang, R. H. Deng, E. Bertino, and D. Zheng, "Robust and Universal Seamless Handover Authentication in 5G HetNets," *IEEE Trans. Dependable Secur. Comput.*, vol. PP, no. c, p. 1, 2019, doi: 10.1109/TDSC.2019.2927664

[38] M. Hojjati, A. Shafieinejad, and H. Yanikomeroglu, "A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks," *IEEE Access*, vol. 8, pp. 216461–216476, 2020, doi: 10.1109/ACCESS.2020.3041710

[39] Y. Xiao and Y. Wu, "5G-IPAKA: An Improved Primary Authentication and Key Agreement Protocol for 5G Networks," *Inf.*, vol. 13, no. 3, pp. 1–17, 2022, doi: 10.3390/info13030125

[40] M. V. Ranjith Kumar and N. Bhalaji, "Blockchain Based Chameleon Hashing Technique for Privacy Preservation in E-Governance System," *Wirel. Pers. Commun.*, vol. 117, no. 2, pp. 987–1006, 2021, doi: 10.1007/s11277-020-07907-w

[41] H. Krawczyk, "Chameleon Hashing and Signatures 1 Introduction," *New York*, no. October, pp. 1–22, 1997.

[42] M. Khalili, M. Dakhilalian, and W. Susilo, "Efficient chameleon hash functions in the enhanced collision resistant model," *Inf. Sci. (Ny).*, vol. 510, pp. 155–164, 2020, doi: 10.1016/j.ins.2019.09.001

[43] J. Xu, H. Chen, X. Yang, W. Wu, and Y. Song, "Verifiable image revision from chameleon hashes," *Cybersecurity*, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00097-3

[44] R. Zhang, "Tweaking TBE / IBE to PKE Transforms with Chameleon Hash Functions," pp. 323–339, 2007.

[45] M. A. Mohamed, "A survey on elliptic curve cryptography," *Appl. Math. Sci.*, vol. 8, no. 153–156, pp. 7665–7691, 2014, doi: 10.12988/ams.2014.49752

[46] A. H. Koblitz, N. Koblitz, and A. Menezes, "Elliptic curve cryptography: The serpentine course of a paradigm shift," *J. Number Theory*, vol. 131, no. 5, pp. 781–814, 2011, doi: 10.1016/j.jnt.2009.01.006

[47] M. Amara and A. Siad, "Elliptic Curve Cryptography and its applications," *7th Int. Work. Syst. Signal Process. their Appl. WoSSPA 2011*, pp. 247–250, 2011, doi: 10.1109/WOSSPA.2011.5931464

[48] Y. Cho et al., "A Secure Three-Factor Authentication Protocol for E-Governance System Based on Multiserver Environments," *IEEE Access*, vol. 10, no. July, pp. 74351–74365, 2022, doi: 10.1109/ACCESS.2022.3191419

https://doi.org/10.59222/ustjet.2.2.2