International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A systemetic Review on Security, Strength and Core of 5G

Anju V. Kulkarni[1], Smitha Sasi*[2], Radhika Menon[3], Mithra Venkatesan[4]

Submitted: 22/08/2023 **Revised**: 07/10/2023 **Accepted**: 20/10/2023

Abstract: The creation of next-generation wireless networks is projected to provide rapid connectivity and low-latency connections in daily life. As a result, network security is essential. The increase in gadgets and the range of facilities that 5G provides have made the environment for network security more difficult. This is exactly it's so important to go to work on workable security solutions right away. The findings of our analysis have demonstrated the several ways that modern wireless network growth will take. Artificial intelligence and software-defined mobile networks are two of them.

Keywords: *5G, Security, Networks security, Privacy, Security challenges, IoT*

1. Introduction

The invention of 5G, the newest advancement in wireless communication technology, is a result of how mobile communication has changed. With multimedia communication now considered basic purposes in our interconnected world, 5G offers new use cases for both clients and businesses, improving the overall quality and usability of communication. Additionally, as 5G permits the networking and interaction of hundreds of millions of devices, it is anticipated that it will open up new economic prospects in the near future. As a result, end users, devices, and 5G infrastructures will all need to meet higher standards for security. The discrepancy between 5G and its forerunners is 5G is a modular system that allows for the simultaneous development of services and structures with various features.For instance, businesses can purchase 5G licenses with geographical restrictions and build unique virtual networks within publicly accessible facilities. Virtual networks and services can constructed and built with particular needs, such as low latency times or high security levels, under the "network slicing" architecture. This presents a chance to create a network that is more dependable, resilient, and secure.

The implementation of 5G technology is expected to eliminate the security gaps present in earlier mobile communication technologies in the upcoming years. These upgrades include improved cryptography, safe moving around, and extensive safeguards to protect signals between different cell networks. In the future, only encrypted data will be used to convey mobile device identifiers, guaranteeing their security from attacks.

[1,2]Department of Electronics and Telecommunication Engineering, Dayananda Sagar College of Engineering,Bangalore India
[3] Department of Mathematics,Dr D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune,India
[4]Department of AI and Data Science,Dr D.Y.Patil Institute of Engineering and Technology,Pimpri,Pune,India
** Corresponding Author Email: smitha.sasi24@gmail.com*

In the future, mobile device identities will only be transmitted in an encrypted format, ensuring protection against attacks. This step is a significant advancement toward creating a secure and reliable mobile communication system, where users can carry out their activities without worrying about potential security breaches. With 5G, users can have peace of mind, knowing that their mobile devices are more secure than ever before. The various research papers suggested several techniques that can help visually disabled people by using voice assistants to detect objects, converts text into speech, provides a description of the images, provides navigation, and so on.

2. Important Security Factors to be Taken Into Account When Standardizing, Developing, Deploying, and Operating Telecommunication Networks.

Since the introduction of international cellular networks like GSM or 2G, standardization has been a crucial component. To maintain seamless network interoperability and security against malicious actors, operators and vendors must cooperate in this process.

The process of standardization also makes agreed-upon security solutions transparent by defining the use of dependable security architectures, protocols, and algorithms.

The network architecture is configured to meet a specific security level defined by the network operator. To ensure network resilience, security parameters are established, and the network is further hardened against attacks. The standardization process plays a crucial role in ensuring that mobile networks are secure, reliable, and trusted, providing users with a seamless and safe communication experience.

Mobility and interoperability are essential elements, but other features, including value-added services, may vary from provider to vendor. Manufacturer implementations'

quality and security might vary, and vendor competition is a key factor in driving up product-level security. For a product to succeed in the market, high product security assurance is essential. The vendor's software development process includes a step called security assurance that includes several lower-level processes to make sure the product only performs as intended.

These sub-processes include, for example, vulnerability evaluation, penetration testers, risk assessment, and privacy impact assessment. In order to verify that the product fulfills industry standards and customer expectations, security assurance may involve third-party audits and certifications in addition to internal efforts. To keep mobile networks secure, foster customer confidence, and increase network dependability, a thorough security assurance methodology is necessary.

3. Hazards Telecom Networks Experience Normally

The number of cyber security threats has grown recently in a variety of sectors, including the telecommunications sector. An increasing number of assaults and attempted attacks have harmed the infrastructure's availability, confidentiality, and integrity. These attacks are frequently made possible by uncomplicated security mistakes such incorrect configuration, hardening, and use of obsolete and vulnerable software versions. However, telecom networks are a particular threat since they have customized specialist equipment that can be attacked by advanced malware. For instance, gaining access to a telecom network's billing and charging system might help insiders with ulterior motives conduct fraud.

Another common group of attackers are hacktivists, who want to stop services, alter websites, or steal private data for financial gain. Another common category of attackers is insider threats, which include resentful former workers or employees who want to take advantage of their trusted position for personal gain. Because they collect and transmit sensitive information, including texts and voice conversations, as well as location data, telecom networks are a desirable target for high-value targets.

New security difficulties are brought on by the frequent connectivity of mobile devices to 5G networks. Attacks including impersonation, eavesdropping, man-in-the-middle, denial-of-service, replay, and repudiation attacks may be possible against social nodes, or the nodes that mobile devices connect to. To stop harmful data from entering the device and spreading throughout it, it is crucial to keep the QoS at a high level and transfer data with little latency. The requirement for high levels of confidentiality in 5G networks makes this task even more difficult. Because of this, attaining zero latency requirements for communications in privacy-preserving 5G networks is a challenging issue.

Security & Privacy Requirements

Because so much sensitive data is sent via telecom networks, including 4G and 5G networks, the highest level of security and privacy is required.

A 5G network must meet several security and privacy requirements, including non-repudiation, deniability, privacy models, confidentiality, integrity, dependability, secure routing transmission, and authentication models.

Through the usage of authenticating and confidentiality techniques, 35 attacks on 4G and 5G cellular networks have been analyzed and prevented, as recorded in the literature. Various standards, like passive attack / active attacks and internal or external attacks, have been used in the literature to categorize hazard replicas in cellular networks.

various categoriesof attacks against as given below,

• privacy

• integrity

•availability

•authentication

Attacks against privacy:

These fourteen attacks on cellular networks are examined and categorised, and include tracking, parallel session, replay, Man-In-The-Middle (MITM), impersonation, collaboration, tracing, spoofing, privacy violation, adaptive chosen ciphertext, chosen-plaintext, stalking, masquerade, and disclosure attacks.

The MITM assault is the most harmful of these. As the suggestion given by Conti et al., the MITMA in wireless networks is primarily constructed on a False Base Station (FBS) assault, in which an evil third party poses as the BTS of an actual network. The use of a temporary confidential channel, a unified cryptographic authentication protocol framework, an entity authentication protocol, password authentication, and key agreement techniques that check the timestamp are only a few of the methods that have been suggested to detect and prevent the MITM attack.

Attacks against the integrity

This category includes the following six forms of attacks: spam, message blocking, message cloning, message alteration, message insertion, and tampering. It should be mentioned that spam attacks may also be regarded as availability attacks. Modifying the data shared between 5G access points and mobile users constitutes an attack on integrity. Commonly used hash methods like SHA-1 and MD5 can identify integrity attacks by confirming the right hash value.

Attacks against availability

Cellular networks in 4G and 5G are divided into six categories. First In First Out (FIFO), redirection, physical, skimming, freeriding, and denial of service (DoS) assaults are examples of these. These attacks' main objective is to obstruct the network's normal functioning and make it unreachable.

The FIFO attack is one particular kind of assault that can be carried out by an enemy who has gathered the entry and departing times of the user equipment. Gao et al. suggested a trajectory mix zones graph model to stop this attack.

Another type of attack that affects the availability of the network is the freeriding attack, which decreases the system accessibility of device-to-device (D2D) communication. Zhang et al. proposed a protocol that keeps track of the status of operator equipment and detects the freeriding attack by ensuring reception non-repudiation through key hint transmission.

Attacks against authentication

Authentication methods in 4G and 5G cellular networks employ several defenses to thwart such attacks. These countermeasures can be divided into three categories: Human variables To improve authentication, smartcards, biometrics, and passwords are employed.

Cryptography methods: Public keys, symmetric keys, and unkeyed methods are used to confirm the safety of data exchanged between devices.

Overall, these countermeasures play a critical part in maintaining the security and integrity of authentication and privacy in cellular networks.

4. Security of Data Traffic

Advanced encryption techniques are used to protect data transported within the 5G infrastructure, guaranteeing that gadgets and the network can validate one another through integrity-protected signaling. This means that even if one system component is hacked, the others are still secure. With 5G, the long-term subscriber identity (IMSI) is now sent in an encrypted form. In contrast, this data was transmitted unencrypted through earlier network technologies like 2G, 3G, and LTE. Additionally, a brand-new security feature dubbed "Authentication Confirmation" has been launched, giving users extra security while traveling.

One benefit of 5G is shorter mobility latency since security-related functions are processed in the base station's centralized unit. The use of location-based authentication in safe identity management systems ensures that only authorized consumers have admittance to network amenities. These technologies are based on robust cryptographic primitives and security elements that were previously present in the 4G system.

In the upcoming future, 5G networks will be equipped with more advanced cryptographic algorithms that have a length of 256 bits. This implementation of cryptographic algorithms will help to provide stronger protection against potential cyber-attacks. Nonetheless, it is essential to keep in mind that the implementation of all security features cannot be guaranteed, and the capability of users to effect these security aspects is to be inadequate.

Therefore, users must remain cautious while selecting applications and service providers, particularly when dealing with sensitive data such as personal or corporate information. While 5G offers advanced security mechanisms, it is still uncertain whether all security features will be implemented correctly. The pace of transformation to the 5G infrastructure by mobile operators is also unclear. Although some benefits of 5G, such as faster transmission rates, can be achieved using an LTE network, the new security mechanisms will not be in use **.**The options supported by the operating system on the User Equipment (UE) are likely to be the extent of end users' ability to alter security measures. It's yet unknown if end customers may command their device to only function on a 5G network. Furthermore, 5G will initially cohabit with 4G, which means that any security vulnerabilities related to the 4G standard will transfer to 5G. The incorporation of technologies alike Software Defined Networks (SDN), Network Function Virtualization (NFV), and cloud into its infrastructure is one of the key variances among 5G and its predecessor technologies. The associated security standards, which are already listed in the 5G specifications, must be met by each core component. But all parties involved in the implementation of these security measures must work together to accomplish a thorough fulfillment of all security requirementsEven while 5G networks now exceed the strict security standards mentioned in the specifications, businesses and 5G providers are nonetheless very concerned about the confidentiality, availability, and integrity of customer information, corporate information, and the safety of IT substructures. Therefore, the same security requirements for present exclusive infrastructures should also be taken into account and enforced when it comes to the key 5G technologies like SDN, cloud, slicing, API Gateway, and the automation of services.

5. Public Key Cryptography

In order to address various security concerns and at different levels for 4G and 5G networks, several techniques already exist and others are being explored.

• The public key infrastructure (PKI) (BS) is used in numerous ways to recognise the open access point (AP) or base station.

• Several methods employ the Paillier cryptosystem, which relies on the creation of keys, encryption, and decryption algorithms.

.• The asymmetric computational cost and high computational effort of Rabin's public key cryptosystem characterise it.

• To achieve conditional anonymity, group signatures with verifier local revocation are utilised.

• Because of group signatures, short group signatures are sometimes employed.

Basically, symmetric encryption is used to guarantee user anonymity. A common option for symmetric data encryption in mobile devices is the Advanced Encryption Standard (AES). Normally symmetric key algorithms are much quicker than asymmetric key algorithms, it enables the adoption of an validation protocol for IoT LTE networks that is fully based on single keys. Recent studies, however, have revealed that it is fundamentally impractical to rely entirely on symmetric-key approaches for user anonymity. To maintain location privacy, semantic safe symmetric encryption is also required.

The following section presents a list of authentication and privacy-preserving schemes for 4G and 5G cellular networks. The schemes are categorized into seven types, which include:

- Handover authentication with privacy
- Mutual authentication with privacy
- RFID authentication with privacy
- Deniable authentication with privacy
- Authentication with mutual anonymity
- Authentication and key agrthe eement with privacy
- Three-factor authentication with privacy

Several authentication models have been developed for security purposes in 4G and 5G cellular networks.

The following are the privacy models that were discovered and put to the test for various security protocols for 4G and 5G networks. Each model focuses on a particular threat that is put forward.

Advance in Keyless Cryptography

The term "keyless cryptography" typically refers to secure message transmission that does not involve key distribution in advance or utilizes key-sharing protocols based on physical layer security. Recent research has produced results related to keyless cryptography, including:

Investigation of Shamir's protocol for secure communication and identification of suitable public key algorithms that can be used with this protocol.

Analysis of Dean's and Goldsmith's cryptosystem that employs multiple-input, multiple-output (MIMO) technology to determine the conditions under which this cryptosystem is secure.

Evaluation of the EVS key scheme proposed by D. Qin and Z. Ding, which was found to be insecure.

Security Considerations for a 5G IoT Network

Networks for the IoT offer a platform for data sharing and communication across various interconnected devices. IoT claims correspond to mMTC and URLLC circumstances in a 5G network, and D2D communication security is essential for safeguarding against potential threats. However, IoT devices have inadequate competences with respect to efficiency, retention, and power consumption, necessitating the effective application of security services.

The security considerations for IoT networks are as follows:

Authentication: The most basic and best method for safeguarding D2D communication in the 5G IoT network is proper user authentication. For the network to maintain network security, users' identities must be confirmed.

• Data Integrity and Confidentiality: Because the IoT network transmits sensitive data, integrity and confidentiality are crucial issues. Data confidentiality and integrity can be provided with the aid of message authentication methods, hash functions, and encryption of transmitted data.

• Anonymity: Concealing the originator's identify and private information, such as a location, is referred to as anonymity. It's important to stop attackers from picking on particular users to serve their objectives.

Efficiency:This is the ability of the system to be deployed and to function profitably. When it comes to the IoT network, availability is crucial, and authorized users must have access to the data whenever they need it.

Overall, securing IoT networks requires robust security measures that take into account the unique characteristics of IoT devices and the potential threats to their security.

Encryption is crucial in securing IoT networks, especially since a vast amount of data is being transferred. To address the security challenges inherent in IoT networks, lightweight block ciphers have been developed. Traditional cryptography methods can be costly and inefficient due to the limited resources available to nodes.

Recent research has focused on modifying the original AES algorithm to create a lightweight and faster alternative,

without compromising its security. It has been observed that this modified AES algorithm works well with low-power IoT devices and sensors. The ECC function of the AES-ECC hybrid encryption system has also been optimized based on the features of wireless sensor networks.

Additionally, texture pictures have been encrypted using bit masking and permutation techniques with the Salsa 20/12 stream cipher. This has been implemented as a component of a brand-new 3D object encryption strategy that works in conjunction with current techniques. In comparison to AES, the usage of PLIE in Python has led to quicker encryption times, higher throughput, and less complexity.

Direct device-to-device (D2D)transmission and reception are essential for 5G networks to improve cellular coverage and radio frequency reuse. Autonomous driving necessitates vehicle-to-everything (V2X) connectivity, which particularly calls for D2D communication. However, D2D communication does come with security risks such free-rider attacks, eavesdropping, privacy probing, and impersonation.A portable and secure D2D communication system is required to guarantee safe authentication, data confidentiality and integrity, and anonymity in order to address these security issues.

D2D communication in mobile networks is susceptible to various security issues. The process for communicatiom consists of detection of a device, connectivity setup, and transmission of data . However, if there is no validation procedure to validate device identity during these procedures. The lack of message authentication for message integrity and message encryption for secrecy makes the communication process vulnerable to attacks including impersonation, eavesdropping, privacy sniffing, and location spoofing.

As IoT and 5G networks take off, security concerns become more crucial. IoT related applications commonly deal with complex data because IoT devices consists of fewer resources in terms of efficiency, the memory, and battery power. As a result, handling these security challenges is more challenging because standard security solutions cannot be applied or processed in an efficient manner. IoT applications align with the mMTC and URLLC use cases for 5G networks.

D2D communication is susceptible to a number of security risks, such as:

Attacks involving impersonation: A hacker could pose as a valid user with an uniqueness like an IMSI (international mobile subscriber identification). Implementing proper user authentication is necessary to thwart this attack.

Eavesdropping: In this kind of assault, the perpetrator observes passively as users converse, recording transferred data that could later be fabricated. Data confidentiality and integrity controls must be implemented in order to stop this attack.

Privacy sniffing: Due to the fact that D2D communication broadcasts request messages to adjacent devices, attackers can use this to locate and follow their targets' devices. Devices should utilize an anonymous identity and be properly validated in order to reduce this security risk.

Free riding attack: Selfish devices take advantage of others' data without contributing their own, which reduces system availability owing to energy use. User identification should be controlled and authenticated by a base station in order to counteract this attack.

Location spoofing: A malevolent device can transmit a request communication with faked or misleading position information in order to hinder D2D communication during the device discovery phase. In D2D transmission , request messages should only be handled from trusted devices in order to thwart this attack.

A secure solution with appropriate device authentication is desirable to handle the securityrelated issues related to D2D communication in the 5G IoT network. Furthermore, any solution must be portable due to the resource-constrained nature of many devices.

Use of portable cryptography is one potential answer to this problem. Such cryptography is practical for use on devices with limited resources and can offer the required level of security.

Elliptic curve cryptography (ECC) is an illustration of an asymmetric-key strategy that combines a 256-bit key with a 128-bit cryptographic algorithm. This suggests a smaller key size than the 3072-bit key employed by RSA, the most popular public-key encryption technique at the moment. Elliptic curve Diffie-Hellman (ECDH) and elliptic curve digital signature technique (ECDSA) are two cryptographic methods that make use of ECC. Both ECDH and ECDSA use public-key cryptography, although their objectives are different. ECDSA is a subset of the digital signature technology used for message signing, whereas ECDH is typically used for key exchange.

Numerous lightweight cryptographic technique with associated data ciphers have recently been proposed for symmetric-key algorithms to meet the resource-constrained nature of some devices. The National Institute of Standards and Technology (NIST) is the standardizing these ciphers at the moment. By exploiting a message authentication code (MAC) during the encryption process, AEAD ciphers to secure data confidentiality ,data integrity and authentication.

Overall, these lightweight cryptographic algorithms are crucial for ensuring secure and efficient D2D communication.

6. Existing Research

A protected, lightweight D2D system with numerous sensors was suggested by Mingsheng Cao et al. The system makes use of an acceleration sensor, secure near field authentication, and lightweight key creation and dissemination. RF and audio channels are used to transmit data, and these channels are also used for encryption and decryption.

The elliptic ElGamal encryption, a public key method over the elliptic curve discrete logarithm problem (ECDLP), is used in a publication by Adeel Abro et al. [12] to implement a light-weight authentication method. To share a secret key within a public key infrastructure (PKI), the proposed approach combines ElGamal encryption and ECC to choose a key pair.

Using public key infrastructure with ECC and ElGamal encryption, asir Javed et al. [13] suggested a simple security system. ElGamal is used for encryption and decryption in the method, while ECC is used to generate keys.

A simple and protected D2D communication protocol was created by Atefeh Mohseni-Ejiyeh et al. [14] for use in 5G networks. To demonstrate successful data sharing in their methods, they use a symmetric encryption scheme, message authentication code (MAC), and the use of digital signatures.

Using smartphone sensor behavior analysis, Haowen Tan et al. [15] developed an authentication technique for device-to-device (D2D) communication. For group authentication, the system uses non certificate cryptography, and for continuous authentication, user behavior analysis gleaned in smartphone sensors is used.Sheeba Backia, Mary Baskaran, and associates [16] proposed a supported D2D communication that can be used in 5G networks as a compact key exchange mechanism for LTE. They use symmetric keys with an ECC foundation..

Yunqing Sun et al. [17] suggested a privacy-preserving technique that makes use of an authentication prefix encryption scheme as well as the ECDH key agreement protocol.

The majority of the mentioned surveys use ECC based cryptographic algorithms to provide data confidentiality/integrity. There are certain restrictions since some findings lack anonymity and because some researchers failed to fully take into account the data transmission/reception of D2D communication. Furthermore, none of the existing methods rely on light-weight symmetric encryption algorithms, but only on light-weight public key algorithms.

Internet of Things Networking Using Lightweight Cryptographic Methods in 5G

The term "lightweight cryptography" (LWC) refers to cryptographic methods with little resource consumption and computational complexity. These justifications support the use of LWC in Internet of Things (IoT) networks in areas with limited resources. Low latency, high throughput, diverse network architecture, and extensive network are just a few of the distinctive characteristics of 5G networks. To overcome these difficulties, SDN-IoT, a new network architecture, has evolved. It allows for the management and control of IoT devices with low latency and high throughput. SDN-IoT's installation can secure and manage the enormous volume of data created by mobile applications. SDN-IoT enables network reprogramming according to unique application requirements. Three layers make up the SDN-IoT network: infrastructure, control, and service/application.

Different LWC algorithms, each with pros and cons, are appropriate for various stages of the SDN-IoT network. The many layers of the SDN-IoT network and the implementation of LWC algorithms in both hardware or software environments are important considerations. There are many SDN security architectures and various LWC algorithm performance measurements.

To enhance the security of data transmissions and receptions over smart devices and mobile network in 4G and 5G networks, numerous encryption algorithms have been suggested.

AES Cipher Algorithm

The Advanced Encryption Standard (AES), industrialized by the National Institute of Standards and Technology, was designed for data transmissions in secure manner in smart devices or mobile network base stations in 4G and 5G networks. The AES-128 cipher technique has ten rounds of functions, but AES-192 and AES-256 have twelve and fourteen rounds, respectively. The four mathematical procedures in each round are the SubBytes operations, ShiftRows operations, MixColumns operations, and AddRoundKey operations. The confidentiality /integrity algorithms (EEA2 and EIA2) used in 4G and 5G networks employ the counter mode method (AES-CTR)-based AES-128 cipher algorithm. The AES-128 cryptographic algorithm has been evaluated using the Incredible Differential technique.

SNOW 3G Cipher Algorithm

For encryption for 3G-UMTS, the SNOW 3G cipher's first iteration was employed. This encryption was also used in certain 4G-LTE data security methods, including 128-EEA1 and 128-EIA1 [15]. SNOW 3G cipher scheme has also been proposed in 5G network. A secret key (where K=128 bits) and an IV key (where IV=128 bits) are used in SNOW 3G. The finite state machine (FSM), which is the second module

of SNOW 3G, has two substitution boxes (Sbox 1& Sbox 2 and registers (R#1, R#2, and R#3).

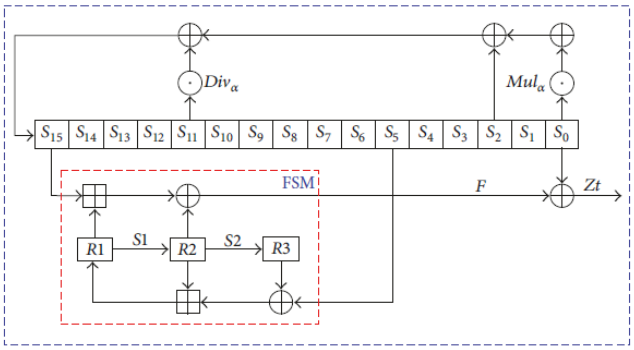

Fig: 1 Design of SNOW 3G Cipher Algorithm

Using a distinctive attack approach applied to the 13 phases of the algorithm, which calls for data complexity and time complexity. Attacking SNOW 3G, which needs 24 bits of approximation and has a complexity of 2172, uses vectorized linear approximations. The IV key and secret key (K) are loaded into the LFSR register during SNOW 3G's startup phase.

ZUC Cipher Alg0rithm

The 4G-LTE network use protected data transmission is using methods like the 128-EEA3 and 128-EIA3, which depend on the ZUC cipher algorithm,. Two keys are needed for the ZUC algorithm: an initialization vector key (IV) and a secret encryption key (K) of 128 bits each. It has mainly three parts: the register LFSR (starts from S0, S1,..., S15), the bit reorganization (BR) (Words: X0, X1, X2, and X3), and the nonlinear function (NLF), which consists of Registers starts from R1 & R2, as well as substitution boxes S-box S0 & S-box S1 [22].

4G systems enabled internet access through mobile broadband networks, providing connectivity between devices and internet were based on two established IEEE standards, WiMAX and LTE. On the other hand, 5G systems are ncorporated more advanced standards and offered additional features, with investigate groups concentrating on improving Dynamic Adhoc Net (DAWN), supporting Voice over IP (VOIP) for voice calls, and enhancing the global wireless web (wwww).

These popular ciphers used in 4G-LTE /5G systems are AES-CTR, SNOW 3G, and ZUC. AES-CTR with 128-bit secret key (K) and initialization vector (IV) for encryption/decryption, making exhaustive key search computationally infeasible shown in Table 1.

Table 1: AES-CTR, SNOW 3G, and ZUC Symmetric Ciphers

	Symmetric Ciphers		
	AES-CTR	SNOW 3G	ZUC
Cipher System	128-bit Block Cipher work in Stream mode	32-bit Word Oriented Stream Cipher	32-bit Word Oriented Stream Cipher
Secret Key	K=128-bit	K=128-bit	K=128-bit
IV Key	IV=128-bit	IV=128-bit	IV=128-bit
Complexity Of Initial Keys	Complexity(K)=2^{128} Complexity(IV)= 2^{128}	Complexity(K)=2^{128} Complexity(IV)= 2^{128}	Complexity(K)=2^{128} Complexity(IV)= 2^{128}
Keystream	128-bit Block	32-bit Word stream	32-bit Word stream
Period of Keystream	2^{64} - 1 Where T0=64-bit	2^{512} - 1 Where LFSR=512-bit	2^{496} - 1, LFSR=496-bit
Structure of Cipher Algorithm	-Bytes Substitution (8-bit S-boxes), -Shift Rows(Byte Permutation.), -Mix Columns (Linear Transform) -Add Round Key	-LFSR (S0,…, S15), -FSM(32-bit registers R1, R2, R3), and -Substitution Boxes (S1,S2)	-LFSR (16 cells), -Bit-Reorganization (128 bits), -Nonlinear Function F(32-bit memory cells R1 and R2), -S-boxes S0 and S1
No. of Rounds	10 rounds	33-steps to produce keystream	33-steps to produce keystream
Cryptanalysis Method	Improved Impossible Differential Cryptanalysis	Chosen IV Cryptanalysis	Differential Cryptanalysis
Mobile Generations	Proposed for security of: 4G-LTE and 5G	Proposed for security of: 4G-LTE and 5G	Proposed for security of: 4G-LTE and 5G

Security in 5G: In the realm of 5G, ensuring security is an increasingly challenging task due to the rapid evolution of communication systems. However, certain security features are always given priority in mobile communication security architectures, such as managing user identities to safeguard identity privacy, implementing mutual authentication between individuals and connections, and utilizing key management and derivation to maintain data confidentiality and integrity.

7. Potential Research Directions

Privacy protection for a 5G radio access network based on the fog paradigm

The 5G radio access network (RAN) can employ the cloud and fog system architecture paradigms to meet the requirements of applications that are mission-critical.

FRAN is a recently proposed integrated RAN design by Ku et al. [24] that blends the two principles. F-RAN includes two methods—loosely-coupled and tightly-coupled—for integrating computer functionality into 5G cellular networks. The privacy of the position and individuality of Fog nodes in the F-RAN architecture could be jeopardized by prospective privacy attacks like man-in-the-middle and replay. Therefore, future work should concentrate on creating privacy-preserving methods for the 5G radio access network that is based on the Fog paradigm.

5G small cell smart grids authentication

Intelligent grid adoption needs a quick and dependable channel, which 5G wireless technology with data and control plane segregation can provide. In order to improve demand response in smart grids and save energy production

costs by up to 30%, researchers have suggested employing advanced multimedia data broadcast and multicasting between tiny cells (aggregators) and smart grid users. The possible impact of network attacks on energy usage, however, is not accounted for in this computation. Despite the fact that a number of authentication techniques have been developed recently to safeguard smart grid communication, they might not be efficient in identifying and thwarting typical assaults or lowering the total cost of production in terms of energy. Consequently, research is required to determine how to lower energy production costs while also minimizing the effects of network attacks.

SDN/NFV architecture with privacy protection in 5G scenarios

The crucial technologies are SDN and NFV , in the opinion of experts, laying the groundwork for the 5G era. It was found that privacy protection had not been considered in any of the modern SDN/NFV mobile packet critical network architectures. Future research in this field could therefore concentrate on the protection of anonymity, location privacy, and identity privacy for this architecture in 5G scenarios. Additionally, in 5G situations, it's critical to ensure authentication among mobile users and devices when implementing SDN/NFV-based collaboration of networks.

UAV privacy-preserving protocols in the 5G network's heterogeneous communication

Unmanned aerial vehicles (UAVs) have a great deal of potential to enhance quality of life in the framework of the IoT through the strategic use of 5G heterogeneous communication settings.. Due to the constraints in wireless communication and computational power, the security and privacy implications of UAV application are complicated. The threat models related to the drone-assisted public safety network were categorized by the authors in a prior study published in 2017 into four categories: attacks on authenticity, availability, secrecy, and integrity. Investigating security techniques for UAV systems for 5G heterogeneous network settings could be a promising research area.

A privacy-preserving authentication system for 5G small cell-based vehicle crowd sensing

User identification and location privacy, among other things, must be protected due to the security issues with vehicular crowdsensing. Investigators have developed a unique strategy for privacy preservation for vehicular crowdsensing using fog computing to overcome these problems. This method makes use of the CLASC certificateless aggregate signcryption algorithm, which claims quick verification and minimal communication overhead.

7. Conclusion and Future Work

Locating the numerous research findings about the security issues surrounding 5G networks that have been made public is the aim of this methodical investigations of the literature.The networks are expected for a variety of services, including health, transportation, and smart cities, based on the quick searches for keywords. These networks' security is crucial because to the nature of the data that is gathered and kept on them. The introduction to the review discussed the development of the cellular networks as well as the 4G and 5G networks.It then focused on the difficulties with 5G network security. The many definitions of cybersecurity and information security were also discussed.The review's primary emphasis was on cyber security .Security concerns at all levels are now more prevalent as a result of the landscape of the 5G network changing. By completing an organized evaluation, the researchers of this study are able to give a comparative analysis of the various security challenges related to 5G networks. 5G networks come with a number of security risks.The review mostly addressed cyber security. Security concerns at all levels are now more prevalent as a result of the landscape of the 5G network changing

References

[1] Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, “An efficient packet parser architecture for software-defined 5g networks,” Physical Communication, vol. 53, p. 101677, 2022.

[2] D. Fang, Y. Qian, and R. Q. Hu, “Security for 5g mobile wireless networks,” IEEE Access, vol. 6, pp. 4850–4874, 2017.

[3] N. Panwar, S. Sharma, and A. K. Singh, “A survey on 5g: The next generation of mobile communication,” Physical Communication, vol. 18, pp. 64–84, 2016.

[4] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5g wireless networks: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.

[5] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, A comprehensive guide to 5G security. Wiley Online Library, 2018.

[6] J. Zhang, W. Xie, and F. Yang, “An architecture for 5g mobile network based on sdn and nfv,” 2015.

[7] P. Schneider and G. Horn, “Towards 5g security,” in 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1. IEEE, 2015, pp. 1165–1170.

[8] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, “Blockchain-enabled authentication handover with efficient privacy protection in sdn-

based 5g networks," IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1120–1132, 2019.

[9] Q. Tang, O. Ermis, C. D. Nguyen, A. De Oliveira, and A. Hirtzig, "A systematic analysis of 5g networks with a focus on 5g core security," IEEE Access, vol. 10, pp. 18 298–18 319, 2022.

[10] R. Dangi, P. Lalwani, G. Choudhary, I. You, and G. Pau, "Study and investigation on 5g technology: A systematic review," Sensors, vol. 22, no. 1, p. 26, 2021.

[11] M. Montano-Blacio, J. Brice ˜ no-Sarmiento, and F. Pes ˜ antez-Bravo, ´ "5g network security for iot implementation: A systematic literature review," in International Conference on Innovation and Research. Springer, 2020, pp. 28–40.

[12] Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, and A. K. Jaiswal, "A systematic literature review on the cyber security," International Journal of scientific research and management, vol. 9, no. 12, pp. 669– 710, 2021.

[13] R. Sethi, A. Kadam, K. Prabhu, and N. Kota, "Security considerations to enable time-sensitive networking over 5g," IEEE Open Journal of Vehicular Technology, vol. 3, pp. 399–407, 2022.

[14] [14] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in Proceedings of the 18th international conference on evaluation and assessment in software engineering, 2014, pp. 1–10.

[15] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," Computers & Security, vol. 88, p. 101629, 2020.

[16] P. V. Torres-Carrion, C. S. Gonz ´ alez-Gonz ´ alez, S. Aciar, and ´ G. Rodr´ıguez-Morales, "Methodology for systematic literature review applied to engineering and education," in 2018 IEEE Global engineering education conference (EDUCON). IEEE, 2018, pp. 1364– 1373.

[17] B. Kitchenham, S. Charters et al., "Guidelines for performing systematic literature reviews in software engineering version 2.3," Engineering, vol. 45, no. 4ve, p. 1051, 2007.

[18] A. Dutta and E. Hammad, "5g security challenges and opportunities: a system approach," in 2020 IEEE 3rd 5G World Forum (5GWF). IEEE, 2020, pp. 109–114.

[19] R. Borgaonkar, I. Anne Tøndel, M. Zenebe Degefa, and M. Gilje Jaatun, "Improving smart grid security through 5g enabled iot and edge computing," Concurrency and Computation: Practice and Experience, vol. 33, no. 18, p. e6466, 2021.

[20] D. Segura, J. Munilla, E. J. Khatib, and R. Barco, "5g early data transmission (rel-16): Security review and open issues," IEEE Access, vol. 10, pp. 93 289–93 308, 2022.

[21] H. Sama, S. Adam, H. Bissa, D. Lamboni, M. Akpanahe, K. Tomta, ` M. Djibril, and M. Gunepin, "Complexite de la cha ´ ˆıne de soutien medical op ´ erationnel au cours d'une mission des nations unies ´ en afrique subsaharienne. a propos d'un cas," ` M´edecine Intensive R´eanimation, vol. 26, no. 6, pp. 528–534, 2017. [22] Q. Qiu, S. Liu, S. Xu, and S. Yu, "Study on security and privacy in 5g-enabled applications," Wireless Communications and Mobile Computing, vol. 2020, 2020. [23] H. Sama, S. Adam, H. Bissa, D. Lamboni, M. Akpanahe, K. Tomta, ` M. Djibril, and M. Gunepin, "Complexite de la cha ´ ˆıne de soutien medical op ´ erationnel au cours d'une mission des nations unies ´ en afrique subsaharienne. a propos d'un cas," ` M´edecine Intensive R´eanimation, vol. 26, no. 6, pp. 528–534, 2017.

[22] "The human central nervous system, 4th ed." May 2008. [Online]. Available: http://www.ajnr.org/content/29/5/e39 [25] E. Zeydan, O. Dedeoglu, and Y. Turk, "Performance monitoring and evaluation of fttx networks for 5g backhauling," Telecommunication Systems, vol. 77, no. 2, pp. 399–412, 2021.

[23] M. T. Raliile and T. C. Haupt, "Application of artificial intelligence for construction workers wellbeing in south africa," in Construction in 5D: Deconstruction, Digitalization, Disruption, Disaster, Development. Springer, 2023, pp. 125–135.

[24] T. Mohammed, A. Albeshri, I. Katib, and R. Mehmood, "Ubipriseq—deep reinforcement learning to manage privacy, security, energy, and qos in 5g iot hetnets," Applied Sciences, vol. 10, no. 20, p. 7120, 2020.

[25] M. Geller and P. Nair, "5g security innovation with cisco," Whitepaper Cisco Public, pp. 1–29, 2018.

[26] Y.-B. Lin, T.-J. Huang, and S.-C. Tsai, "Enhancing 5g/iot transport security through content permutation," IEEE Access, vol. 7, pp. 94 293–94 299, 2019.

[27] K. F. Jasim, K. Z. Ghafoor, and H. S. Maghdid, "Analysis of encryption algorithms proposed for data security in 4g and 5g generations," in ITM Web of Conferences, vol. 42. EDP Sciences, 2022, p. 01004.

[28] R. F. Olimid and G. Nencioni, "5g network slicing: A security overview," IEEE Access, vol. 8, pp. 99 999–

100 009, 2020.

[29] R. Sethi, A. Kadam, K. Prabhu, and N. Kota, "Security considerations to enable time-sensitive networking over 5g," IEEE Open Journal of Vehicular Technology, vol. 3, pp. 399–407, 2022.

[30] X. Zhang, A. Kunz, and S. Schroder, "Overview of 5g security in ¨ 3gpp," in 2017 IEEE conference on standards for communications and networking (CSCN). IEEE, 2017, pp. 181–186.

[31] Q. Qiu, S. Liu, S. Xu, and S. Yu, "Study on security and privacy in 5g-enabled applications," Wireless Communications and Mobile Computing, vol. 2020, 2020. [35] A. Afaq, N. Haider, M. Z. Baig, K. S. Khan, M. Imran, and I. Razzak, "Machine learning for 5g security: Architecture, recent advances, and challenges," Ad Hoc Networks, vol. 123, p. 102667, 2021.

[32] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu et al., "Overview of 5g security technology," Science China Information Sciences, vol. 61, no. 8, pp. 1–25, 2018.

[33] S. Kwon, S. Park, H. Cho, Y. Park, D. Kim, and K. Yim, "Towards 5g-based iot security analysis against vo5g eavesdropping," Computing, vol. 103, no. 3, pp. 425–447, 2021.

[34] J. Zhang, Z. Yan, S. Fei, M. Wang, T. Li, and H. Wang, "Is today's end-to-end communication security enough for 5g and its beyond?" IEEE Network, vol. 36, no. 1, pp. 105–112, 2021.

[35] E. U. Ogbodo, A. M. Abu-Mahfouz, and A. M. Kurien, "A survey on 5g and lpwan-iot for improved smart cities and remote area applications: From the aspect of architecture and security," Sensors, vol. 22, no. 16, p. 6313, 2022.

[36] B. Manale and T. Mazri, "Security of communication 5g-v2x: A proposed approach based on securing 5g-v2x based on blockchain," in ITM Web of Conferences, vol. 43. EDP Sciences, 2022, p. 01025.

[37] K. Saleem, G. M. Alabduljabbar, N. Alrowais, J. Al-Muhtadi, M. Imran, and J. J. Rodrigues, "Bio-inspired network security for 5g-enabled iot applications," IEEE Access, vol. 8, pp. 229 152– 229 160, 2020.

[38] F. Salahdine, T. Han, and N. Zhang, "Security in 5g and beyond recent advances and future challenges," Security and Privacy, p. e271, 2022.

[39] M. Attaran, "The impact of 5g on the evolution of intelligent automation and industry digitization," Journal of Ambient Intelligence and Humanized Computing, pp. 1–17, 2021.

[40] A. Makkar, "Enhancing iot security using 5g capabilities," 2021.

[41] P. Varga, J. Peto, A. Franko, D. Balla, D. Haja, F. Janky, G. Soos, D. Ficzere, M. Maliosz, and L. Toka, "5g support for industrial iot applications—challenges, solutions, and research gaps," Sensors, vol. 20, no. 3, p. 828, 2020

[42] Sarangi, D. P. K. . (2022). Malicious Attacks Detection Using Trust Node Centric Weight Management Algorithm in Vehicular Platoon. Research Journal of Computer Systems and Engineering, 3(1), 56–61. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/42

[43] Balasubramanian, S. ., Naruka, M. S. ., & Tewari, G. (2023). Denoising ECG Signal Using DWT with EAVO . International Journal on Recent and Innovation Trends in Computing and Communication, 11(3s), 231–237. https://doi.org/10.17762/ijritcc.v11i3s.6184