Security of IoT in 5G Cellular Networks: A Review of Current Status, Challenges and Future Directions

Hemangi Goswami and Hiten Choudhury

Department of Computer Science and Information Technology, Cotton University, Assam, India

***Abstract*:** The Internet of Things (IoT) refers to a global network that integrates real life physical objects with the virtual world through the Internet for making intelligent decisions. In a pervasive computing environment, thousands of smart devices, that are constrained in storage, battery backup and computational capability, are connected with each other. In such an environment, cellular networks that are evolving from 4G to 5G, are set to play a crucial role. Distinctive features like high bandwidth, wider coverage, easy connectivity, in-built billing mechanism, interface for M2M communication, etc., makes 5G cellular network a perfect candidate to be adopted as a backbone network for the future IoT. However, due to resource constrained nature of the IoT devices, researchers have anticipated several security and privacy issues in IoT deployments over 5G cellular network. Off late, several schemes and protocols have been proposed to handle these issues. This paper performs a comprehensive review of such schemes and protocols proposed in recent times. Different open security issues, challenges and future research direction are also summarized in this review paper.

***Keywords*:** Internet of Things, IoT, 5G Cellular Networks, Security, 3GPP, M2M Communication**.**

1. Introduction

Internet of Things (IoT) refers to the collection of different interconnected heterogeneous objects and devices in an internet like architecture to communicate among themselves. These uniquely identifiable physical objects are expressed with their virtual representation to achieve a common goal in different areas and applications [1]. In various applications like agriculture [2], healthcare [3], transportation [4], Smart Home [5], Smart Cities [6], etc., IoT technology is being widely used [7]. Therefore, IoT has become a focus of research in different industry applications like cyber-physical systems (CPS), machine to machine (M2M) communications, cyber-transportation systems (CTS) etc. Figure 1 shows the architecture of the Internet of Things.

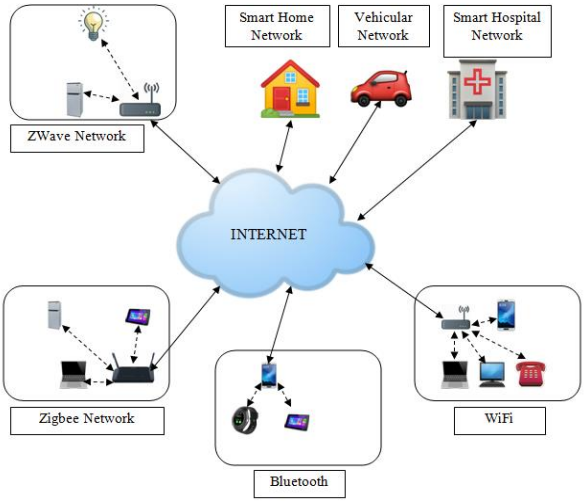

Figure 1: Architecture for Internet of Things

After successful implementation of 4G, 5G is being developed as an evolved platform of 4G with several additional advantages and features. Since 3GPP based LTE is one of the most successful cellular networks, 3GPP 5G is also expected to reach the same level. 5G network introduces several advantages like high bandwidth, faster communication, wider coverage, easy and cost-effective connectivity, machine type communication etc., and thus has all the versatility to be adopted as the backbone network for the future IoT. However, successful implementation of IoT over 5G depends how well the security issues are addressed. With the advancement of modern-day cellular networks, new security and privacy concerns are emerging. Moreover, the use case scenarios of IoT over cellular networks are numerous; for instance: healthcare management system, smart home management system, transportation system, power grid management system, smart metering, etc. Therefore, different use case scenarios will require different security solutions that takes the resource constraints of an IoT environment into consideration. Several schemes and protocols have been proposed in recent times to handle the above discussed issues.

The main focus of this paper is to give a comprehensive idea about the authentication schemes and security solutions proposed for an IoT environment with 5G cellular network as a backbone. Additionally, different security-based challenges and threats that need to be considered in an IoT environment are discussed in this paper. Furthermore, based on the open issues, future research directions are also highlighted. In the literature, there are several papers present in the area of IoT in general. But there are not too many survey papers that describe the authentication mechanism for IoT over 5G cellular networks [8] [9] [10].

Contribution and Approach - The contributions of this paper are as follows.

- The advantages of IoT over 5G cellular network are highlighted.
- The security mechanism in 5G cellular network is presented.
- The security issues and threats for IoT in 5G cellular network are highlighted.
- Schemes and solutions proposed recently to tackle security issues/threats in IoT over 4G/5G cellular network are studied and compared with each other. Such solutions may contribute in providing valuable insights for designing future solutions.
- Various techniques used in the above schemes are highlighted.
- Computation/Communication cost of implementation of the above proposals in the resource constrained IoT environment are calculated and highlighted.
- Based on the study of the recent proposals, gaps in research were identified and future research directions

for improved security in IoT over 5G cellular network are discussed.

Organization of the Paper - The paper is organized as follows – Section 2 illustrates the overview of IoT in 5G cellular network. Security mechanism in 5G cellular network is described in Section 3. In Section 4, different security issues and threats in 5G-IoT is discussed. Section 5 describes the solutions or methods available in the literature for addressing/ overcoming the security issues and threats in 5G IoT. Section 6 presents a discussion on the future research directions. Finally, the paper is concluded in Section 7.

2. Overview of IoT in 5G Cellular Networks

5G IoT comprises of interconnected heterogeneous objects and devices like RFID (Radio-Frequency Identification Device), sensors, actuators and cellular phones, that communicate among themselves through the 5G cellular network. These uniquely identifiable physical objects collect information from their environment and communicate among each other to achieve a common goal in different areas of applications [11]. 5G IoT is set to revolutionize several aspects of our day- to-day activities as depicted in Figure 2. Many processes around us are going to be automated, making them fast and much more efficient. Some of the use cases of 5G IoT are as follows.

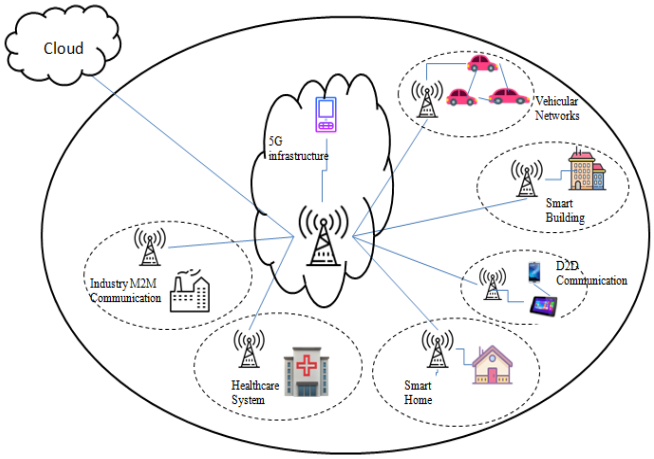

Figure 2: Architecture for 5G-IoT

Health Sector: In the health sector, 5G IoT may play an important role with its long-distance full duplex communication link [3]. In the remote areas, efficient patient monitoring may be done using e-healthcare system. Using 5G communication link, patient's vital signs may be transmitted from one hospital to another major hospital. Doctors from the major hospitals can monitor and diagnose patient's vital signs and can send back the results using the same communication link.

Smart Home: Smart home [5] is one of the major applications in 5G IoT system. Different household appliances may be connected through the 5G network to communicate among themselves without human interruption. Home appliances such as refrigerator, AC, T.V, and every electronics gadget may be connected to the internet for smooth and efficient functioning. Future houses will be constructed with smart windows and doors which operate with the internet connectivity and the electronics equipment such as smart sensors and remote control. Overall, 5G cellular networks will enable appliances and devices to talk among themselves and it will enable the devices to pass information at high speed to locations where decisions may be taken.

Transportation Sector: Use of IoT in transportation sector will result in Intelligent Transportation System (ITS) [4]. In Future intelligent transport management systems, control system and communications networks will be integrated together to make transportation systems more reliable, efficient and secured. In future transportation systems, each smart vehicle will be deployed with smart sensors and electronic control unit to monitor and control the vehicle. Smart cars will have 5G radars, which will use mm wave technology that propagates through fog and rainy condition, for providing collision avoidance systems (CAS) and automatic brake system (ABS). With these communication interfaces, there will be communication between vehicle to vehicle (V2V) and vehicle to anything (V2X). Every vehicle in IoT networks will be connected to the intelligent transportation systems for exchange of information, traffic status and road conditions for prevention of major accidents and will provide more secured travels to the passengers.

Agriculture Sector: At the agriculture front, power sector, supply chain management, etc., IoT has brought in technologies like smart metering, smart grid, etc., which can play a very important role in the pervasive computing environment [2].

In IoT, the things or devices may be connected with each other through modern communication technologies like the following.

ZigBee: It is a low power wide area network, which is an extended version of IEEE.802.25.4 that is used for communicating in a pervasive computing environment. Due to its simplicity and low cost, it is widely used in home automation, healthcare, industrial IoT etc. within a range of 100m [12].

Bluetooth Low Energy (BLE): It is a wireless PAN (Personal Area Network) technology that is used in different applications like healthcare system, security, home entertainment industries etc. It can provide considerably reduced power consumption and cost compared to the classic Bluetooth system [13].

Low Power -Wi-Fi, Low Power Wide Area (LPWA): They are based on 802.11 standards and is used in machine type communication and short-range communication i.e., Local Area Network (LAN). It operates in a Transmission range of Wi-Fi is 100m and frequency band of 2.4-5 GHz [14].

5G Cellular Network: It is recent communication technology that is set to revolutionize IoT in terms of speed of communication, flexibility, availability, etc., is the 5G cellular technology. As the cellular network technology is evolving from their fourth generation to fifth generation, 5G network introduces several advantages like high bandwidth, ultra-high bit rate, wider coverage, easy connectivity, massive device connectivity, machine type communication etc and thus have all the versatility to be adopted as the backbone network for the future IoT. Thus, 3GPP based 5G can be considered as the future telecommunication system that can support massive Machine Type Connectivity (mMTC) [15]. In spite of the above advantages, there are several challenges of IoT in 5G Cellular Network, which are listed as follows.

- Energy constraints of the IoT devices.
- Processing constraints of the IoT devices.
- Providing security to the resource constrained IoT devices.

A detailed discussion of the various security challenges and threats for IoT in 5G cellular network is presented in Section 4.

3. Security in 5G Cellular Networks

In this section, we present the security architecture of the 5G cellular network and the authentication and key agreement protocol that is used for access security.

3.1 Authentication and Key Agreement in 5G Cellular Network

In this section, we highlight the authentication and key agreement protocol used for access security in 5G cellular network. As shown in figure 3. 5G authentication and Key Agreement (5G-AKA) protocol was standardized by 3GPP, where three main components are involved: the User Equipment (UE), that contains a Universal Subscriber Identification Module (USIM); the Home Network (HN), that comprises of the Unified Data Management (UDM), the Authentication Credential Repository Function (ARPF) and the Authentication Server Function (AUSF); and the Serving Network (SN), that comprise of Access and Mobility Management Function (AMF) and the Security Anchor Function (SEAF) [16]. The USIM contains the Subscription Permanent Identifier (SUPI) which is a unique and permanent subscriber identity, the HN's public asymmetric key 'pkHN', a long-term shared symmetric key 'K' and a sequence Number 'SQN'. The SUPI is encrypted using the home network's public key to form Subscription Concealed Identifier (SUCI).

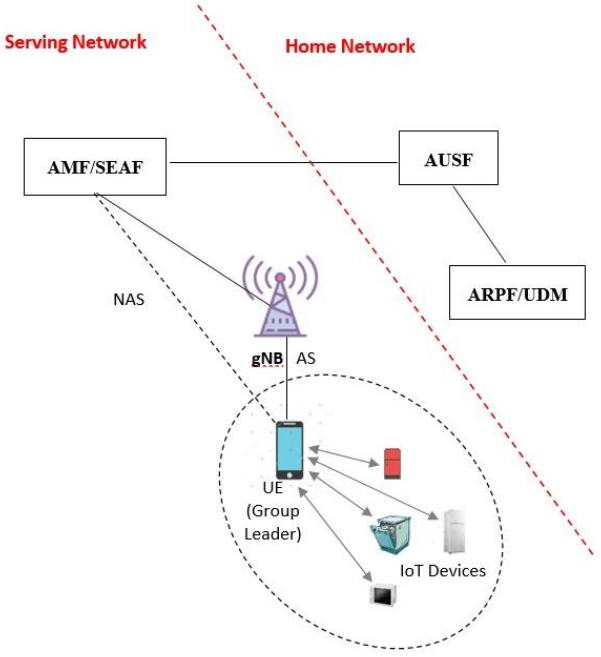

Figure 3: Security architecture of 5G-IoT

The 5G Authentication and Key Agreement (5G-AKA) protocol [16], standardized by 3GPP, consist of the following steps [17] [7].

i. UE transmits Globally Unique Temporary Identifier or encrypted SUCI to the serving network.
ii. Serving Network, i.e., SEAF sends a request to AUSF for authentication.
iii. AUSF then sends the authentication request to UDM/ARPF.
iv. If AUSF received SUCI, it decrypts SUCI to SUPI using the Subscription Identifier De-Concealing Function (SIDF) to identify the shared secret key 'K'. Then, UDM/ARPF generates the Authentication Vectors (AV's) consisting of an Authentication token (AUTH), Expected Response (XRES), a Key (K_{AUSF}) using the key 'K' and a set of one-way hash function.
v. The Authentication response is then transmitted to AUSF consisting of Authentication Vector along with the SUPI.
vi. AUSF then stores the key K_{AUSF} and generates the hash value of XRES(h(XRES)).
vii. AUSF transmits authentication response to SEAF that contains AUTH and h(XRES). SUPI is not sent to the SEAF along with the response. It is sent after successful completion of the UE authentication.
viii. After storing the h(XRES), SEAF send an authentication request (AUTH) to UE.
ix. Using the shared secret key 'K', UE validates the AUTH. If validation is successful, then UE considers that the serving network is authenticated.
x. UE computes the response value (RES) and send it to SEAF.
xi. SEAF computes the hash of the RES value and compares it with the stored h(XRES) value.
xii. SEAF also send the RES to AUSF to validate the value.
xiii. AUSF validates the RES value with the stored XRES value. If validation is successful, then AUSF computes the anchor key K_{SEAF} using K_{AUSF}.
xiv. K_{SEAF} is then transmitted to SEAF from AUSF along with SUPI.
xv. Finally, AUSF also informs ARPF/UDM that the authentication is successful. [52] [53]

The following figure (Fig 4) shows the Authentication and Key Agreement protocol in 5G cellular network.

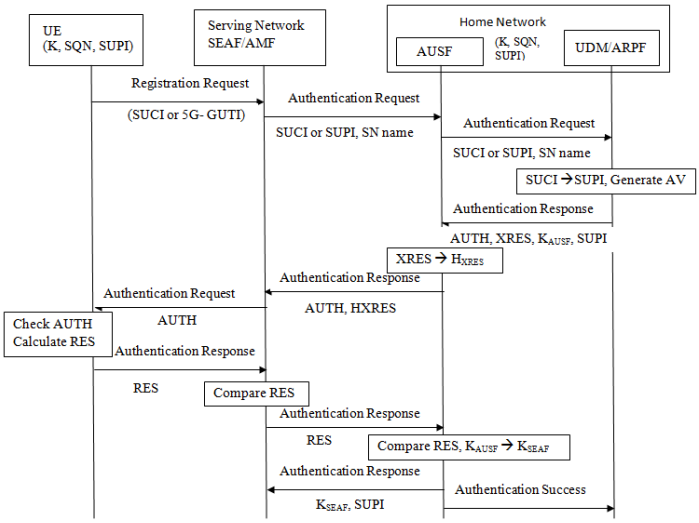

Figure 4: 3GPP 5G-AKA

The hierarchy for key generation in 3GPP-5G AKA protocol is shown in the Figure 5 [19][20]. The integrity and confidentiality keys are derived from the key K_{gNB}. Final key sets that are generated after successful completion of 5G Authentication and Key Agreement protocol and their detailed usage are describes as follows.

- K_{RRCint}: used in Radio Resource Control Integrity protection.
- K_{RRCenc}: used in Radio Resource Control encryption.
- K_{UPint}: used in user plan integrity protection.
- K_{UPenc}: used in user plan encryption.

- K_{NASint}: used in Non-Access Stratum (NAS) Integrity Protection.
- K_{NASenc}: used in Non-Access Stratum encryption.

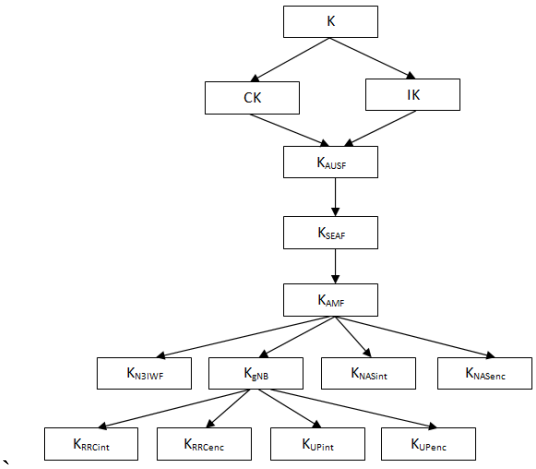

Figure 5: Keys generated during 3GPP 5G-AKA

4. Security Issues and Threats for IoT in 5G Cellular Networks

The User Equipment (UE) or a smart phone is designed to be carried around for the convenience of a user, so that he/she may have access to various data and voice-based services. A single subscriber usually possesses a single or a limited number of smart phones. However, in case of IoT devices the scenario changes completely. A subscriber may have possession of hundreds of IoT devices that are hooked on to the Internet. Therefore, exposing the subscriber to various known and unanticipated threats. Each IoT device may give out crucial private information about the day-to-day activities of the subscriber. In this section, we discuss some of the security issues and threats that a subscriber may have to face while s/he is connected to the IoT through the 5G cellular network.

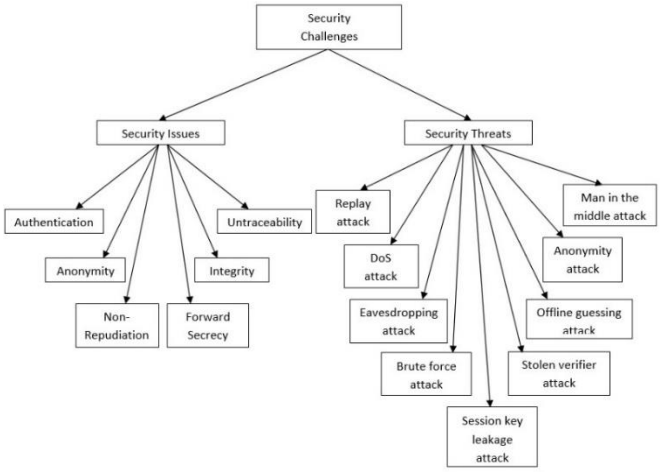

Figure 6: Security issues and threats present in IoT 5G.

4.1 Security Issues

Different security issues that should be considered in a 5G-IoT environment are as follows [18].

- *Authentication* – It is the process of verifying whether a particular device is a genuine registered device or not. It is important to ensure that before extending any service (voice based or data based), a device is duly authenticated.
- *Anonymity* – It is important that during IoT communications, the identity of the individual who owns the IoT devices does not get revealed. The anonymity and privacy of the individual should be respected.
- *Integrity* – It should be ensured that the data and information exchanged in the IoT environment should not be altered or modified in transition.
- *Authorization* – It should be ensured that only data originated at authorized or authenticated nodes be considered for further processing.
- *Non-Repudiation* – It is important that no stakeholder in the IoT environment is able to deny transmitting a message that was originally send by it.
- *Data freshness* – There should be mechanism to validate the freshness of received data. So that protection from replay attack may be ensured.
- *Forward secrecy* – It is important that no adversary can relate two different sessions with each other. It should be ensured that session keys are not compromised even if long term secrets used in the session key exchange are compromised.

4.2 Security Threats

Several attacks are possible in an IoT environment. Some of the well-known attacks are as follows [15].

- *Masquerade attack*: In this attack, an adversary uses fake identity to authenticate himself as a legitimate user in that IoT environment. Some of the examples of this type of attack are - impersonation attack, anonymity attack, user tracking attack, identity theft attack, insider attack, stolen verifier attack.
- *Man-in-the-middle attack*: In this attack, an attacker secretly gains access to the network and possibly modifies the communication between two parties who believe that they are communicating directly with each other. Examples of MITM attack are - eavesdropping attack, substitution attack, message modification attack, false message attack, data manipulation attack, password updating attack, session key leakage attack, etc.
- *Denial-of-service attack*: In this attack, the attacker tries to make a service or resource unavailable by creating a huge amount of traffic at a time so that genuine user can't access the services. Some examples of DoS attack are - Distributed DoS attack, rejection attack, desynchronization attack, etc.
- *Forging attack*: In this attack, the attacker uses authenticated data of a legitimate user illegally to access the service of the network. Examples are - gateway forgery, sensor forgery, replay attack, collusion attack, white and black box attack, etc.
- *Guessing attack*: In this attack, an attacker tries to guess the authentication credentials i.e., user id, password, secret key, etc., when they can't extract that information physically. Some examples of guessing attack are - chosen plain text attack, brute-force attack, offline guessing attack, social networking attack, etc.
- *Physical attack*: In this attack, the IoT devices are accessed physically by the attackers. In the network, thousands of IoT devices are present and it is not possible to protect all the devices physically. Examples of physical attack are - cellular device loss, stolen card attack, USB attack etc.

- *Routing attack*: In this attack, data and information are transmitted illegally from non-legitimate user to some improper destination. Examples are - sinkhole attack, wormhole attack, black hole attack, link ability attack, etc. Figure 6 shows different types of security issues and threats that can be present in an IoT environment over 5G cellular network. Addressing the issues and detecting the attacks and protecting the environment from these attacks is a very challenging task in the IoT environment.

5. Recent proposals in the Literature

In this section, we present some of the recent works in the literature proposed for resolving the Issues and Threats in IoT over 5G cellular networks. Some of the techniques that are used to resolve the issues and the threats in the various proposals are discussed as follows (Figure 7).

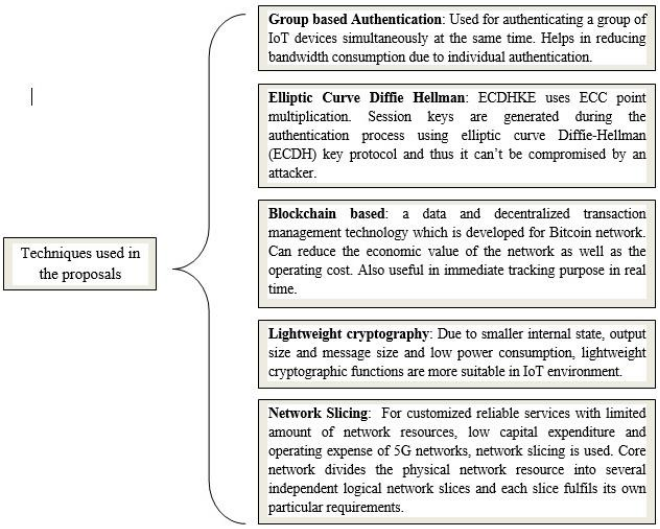

Figure 7: Technique used in the proposals.

1. *Group Based Authentication:* In group-based authentication, a group of IoT devices is formed and a GROUP LEADER is selected from the group. When the IoT devices want to communicate with some other device through the core 5G network, a signature and an encrypted information are sent to the group leader by the IoT device. After receiving the encrypted data, group leader aggregates the information and send the encrypted data to the 5G core network. 5G network then verify the validity of the IoT device group. Again, the network is also verified by the device group so that mutual authentication can be achieved. In case of cellular network, all cellular system has a secret identity i.e., IMSI (International Cellular Subscriber Identifier). But, in case of IoT network, it is impossible to assign IMSI number to all the devices connected in the network due to consumption of high bandwidth. Thus, to develop a scheme using group-based authentication is important, where many devices are connected to the network through hotspot and only one device with sim card is connected to the 5G core network. [31], [35] used group-based authentication during their authentication process.
2. *Elliptic Curve Diffie Hellman:* Elliptic Curve Diffie Hellman Key Exchange [61] is similar to the traditional DHKE protocol, but only difference is that instead of using modular exponentiation, ECDHKE uses ECC point multiplication. In this protocol, sender A has a key pair (d_A, Q_A) and receiver B also has a key pair (d_B, Q_B), where d is the private key, Q (=d.G) is the public key and G is the generator point of ECC. Now, for A, QA = d_A.G and for B, Q_B = d_B.G. A computes a point (x_k, y_k) = d_A.Q_B and B computes a point (x_k, y_k) = d_B. Q_B. The point, i.e., shared secret key, calculated by both parties is equal [60].
d_A. Q_B = d_A. d_B. G = d_B. d_A. G = d_B. Q_A
Session keys are generated during the authentication process using elliptic curve Diffie-Hellman (ECDH) key protocol and thus it can't be compromised by an attacker. Thus, to achieve data confidentiality and to prevent the network from Man in the Middle attack, ECDHKE protocol is used. In [31], Elliptic curve Diffie Hellman key exchange is used during the authentication process.
3. *Blockchain:* Blockchain [58] refers to a data and decentralized transaction management technology which is developed for Bitcoin network. The focus in Blockchain [59] for various research areas is increasing due to Different central attributes which can provide Anonymity, Data integrity, Security etc. Blockchain technology along with 5G network can reduce the economic value of the network as well as the operating cost. Blockchain with 5G technology is also useful in immediate tracking purpose i.e., to track the exact location of the user in real time. Double spend problem is eliminated with the help of public key cryptography using Blockchain technology in which a private-public key pair is assigned to every agent and that the public key is shared with all other agents. [32], [37] have used Blockchain based technique during the authentication and key agreement procedure.
4. *Digital Signature:* Digital signature is a type of public key cryptography that is calculated from the message and the signer's secret key or private key and is used to verify the authenticity and integrity of a message. In digital signature, first of all the sender signs the original message with its private key and then send the original message and the signed message to the receiver. Receiver decrypts the signed message with sender's public key and if both the generated and received messages are same then, the author of the message is validated. Digital signature is used in authentication process to achieve integrity of the network. In [31], [35], the authors use digital signature for integrity protection.
5. *Lightweight Cryptography:* Various Lightweight cryptographic Techniques [51] [52] that can be used for authenticating a network are XOR, Lightweight Message Authentication Codes, one way Hash function, Elliptic Curve Cryptography (ECC) etc. Due to smaller internal state, output size and message size and low power consumption, lightweight cryptographic functions are more suitable in IoT environment security control than traditional cryptographic techniques. Using a one-way hash function during authentication can provide untraceability and user anonymity property. ECC is used in resource constraint environment to find the Public Key family with smaller operands. Elliptic Curve, Ep over Fp, (where p is a prime number)

is defined as the mathematical equation, y2=(x3+ax+b) mod p, where (4a3+27b2) mod p != 0. A point, (x,y), (where x, y ∈ Fp) is a point on that curve if the point satisfies the equation y2 = x3+ax+b. Suppose, X is a point present on that curve and R is any random number, then, Q (= X.R), is also a point present on that curve [49] [50]. In [36], [37], [39], Lightweight cryptographic techniques are used for authentication purpose.

6. *Network Slicing:* For customized reliable services with limited amount of network resources, low capital expenditure and operating expense of 5G network, network slicing is used. Here, core network divides the physical network resource into several independent logical network slices and each slice fulfils its own particular requirements. In [34], network slicing is used by the authors.

Table 1: Recent proposals for 5G-IoT vis-à-vis the techniques used for improved security.

Title of the Proposal	Author	Technology Used
Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network	Cao et al. [31]	Group-based Authentication, Elliptic Curve Diffie-Hellman (ECDH) key protocol, Digital Signature
Blockchain-based trusted authentication in cloud radio over fiber network for 5G	Yang et al. [32]	Blockchain
Efficient and Secure Service-oriented Authentication Supporting Network Slicing for 5G-enabled IoT	Ni et al. [34]	Network slicing, Fog Computing, Elliptic Curve Diffie-Hellman Key Exchange Protocol (ECDH), Public key Cryptography
Anti-quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System	Cao et al. [35]	Quantum Cryptography, lattice-based homomorphic encryption, Group based authentication, Digital Signature
LACS: A Lightweight Label-Based Access Control Scheme in IoT-Based 5G Caching Context	Wang et al. [36]	Lightweight Cryptography
Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Cellular Edge Computing Environment	Jangirala et al. [37]	Lightweight Cryptography, Blockchain
Secure Authentication Protocol for 5G Enabled IoT Network	Sharma et al. [38]	Application layer security based,
An Authenticated Key Exchange Protocol for Multi-Server Architecture in 5G Networks	Wu et al. [39]	Cloud Computing, Lightweight Cryptography
Certificateless Multi-Party Authenticated Encryption for NB-IoT Terminals in 5G Networks	Zhang et al. [40]	Multi party authenticated encryption,
HashXor: A lightweight scheme for identity privacy of IoT devices in 5G mobile network	Coudhury et. al. [62]	Lightweight Cryptography: Hash and Xor Operations.
LSAA: A Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks.	Cao et. Al. [63]	Lightweight cryptography: extended Chebyshev chaotic Maps.

Here, we discuss some of the prominent solutions available in the literature for improving security of IoT in 4G/ 5G cellular network. These proposals may help in providing valuable insights into novel approaches and techniques for dealing with security challenges of IoT in 5G cellular network. In recent times, several researchers have proposed novel schemes to tackle security challenges and threats for IoT in 5G cellular networks.

- In [31], Jin Cao et al. have proposed a Fast Authentication and Data Transfer Scheme based on the certificateless aggregation signcryption technique for Massive NB-IoT Devices in 3GPP 5G Network, where elliptic curve Diffie-Hellman (ECDH) key protocol is used to establish the session keys and downlink data are encrypted with the session keys between each IOTDi and MME. According to the authors, this protocol also deals with anonymity, non-repudiation as well as protection against different known attacks. Replay attack by addition of random number, MITM attack by generating the session key, counterfeiting attack because any attacker can't generate the valid aggregate signcryption or digital signature without the private key.
- A Blockchain based trusted authentication scheme for 5G was proposed by Hui Yang et al. in cloud radio over fiber network [32].
- Hussain Al-Aqrabi et al. evaluated an approach for developing a flexible and secure model for authenticating Industrial Internet of Things (IIoT) components in dynamic 5G environments [33].
- In [34], Jianbing Ni et al. proposed an Efficient and Secure Service-oriented Authentication that supports Network Slicing and fog computing for IoT over 5G. Here, three issues are taken care of by the authors – Authentication, Anonymity and Confidentiality. This protocol does not consider roaming services for IoT over 5G that can access the network efficiently.
- Traditional authentication mechanism is used by NarrowBand Internet of Things (NB-IoT) devices for accessing the network and performing mutual authentication with the network, which can produce a huge amount of signaling and communication overhead. Thus, Jin Cao et al. [35] produced a quantum resistant Fast Authentication and Data Transmission mechanism for Massive Devices in 5G NB-IoT System that can protect the network from security and privacy issues and

can reduce the network load. This scheme is based on lattice-based homomorphic encryption technology

- In [36], Qixu Wang et al. has presented a scheme LACS: A Lightweight Label-Based Access Control Scheme in IoT-Based 5G Caching Context that authenticates the authorized fog nodes to ensure protection. The proposed schemes can authenticate the fog nodes by verifying the integrity of the shared files that are embedded label values so that only the authenticated fog nodes can access the caching service.
- In [37], Jangirala et al. has designed a Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains (LBRAPS) in 5G Cellular Edge Computing Environment. This scheme is based on bitwise exclusive-OR (XOR), one-way cryptographic hash function and bitwise rotation operations.
- Suraj Sharma et al. [38] proposed a secure Authentication Protocol for 5G Enabled IoT Network that can protect the network from all those attacks originating from public access network. It is an application layer security protocol and deals with Confidentiality, Integrity and Availability
- In [39], Tsu-Yang Wu et al. have proposed an Authenticated Key Exchange Protocol for Multi-Server Architecture in 5G Networks that deals with perfect forward secrecy (PFS) and privileged insider (PI) attacks and it is claimed by the authors that the protocol achieves higher security standards.
- A Certificateless Multi-Party Authenticated Encryption scheme was proposed by Yinghui Zhang et al. [40] for NB-IoT Terminals in 5G Networks which deals with identity anonymity and non-repudiation. In this scheme access authentication and data transmission are combined into one Process.
- A lightweight scheme, HashXor, for identity privacy of IoT devices in 5G mobile network was proposed by H. Choudhury [62]. It includes two Hash operations and three Xor operations to achieve all the security requirements.
- Jin Cao et al. [63] proposed a lightweight secure access authentication scheme, LSAA, for UE and mMTC devices in 5G mobile network. According to the author, the scheme can achieve several security requirements including anonymity and privacy.

The above discussed authentication protocols and the technology used in these proposals are summarized in Table 1.

5.1 The Proposals vis-a-vis the Security Issues

In this subsection, we elaborate some of the recent proposals in terms of the security issues addressed by them.

- In [31], Elliptic Curve Diffie-Hellman (ECDH) key protocol is used by Jin Cao et al. to establish the session keys and downlink data are encrypted with the session keys between each IOTDi and MME to achieve data confidentiality. Digital signature is used in this scheme to authenticate the MME and to protect the integrity of the downlink data. IoT device's identity and group identity is protected in each session, thereby providing anonymity.
- In [35], Authentication is achieved, because random number is used to generate the signature which can't be generated by the attacker without the correct random number. During the authentication process, the user's identity is not known to anyone and thus preserving the user anonymity. This scheme is based on deterministic Diffie Hellman Problem and therefore it provides data confidentiality to the network. Digital signature is used to achieve integrity of the network.
- In [36], it is claimed by the authors that it can authenticate the fog nodes by verifying the integrity of the shared files that are embedded label values so that only the authenticated fog nodes can access the caching service.
- In [37], bitwise exclusive-OR (XOR), one-way cryptographic hash function and bitwise rotation operations are used by the authors to authenticate the environment. In the scheme, to protect the confidentiality of transmitted data, participants use random numbers for generating the messages such that it is difficult for attacker to extract the original message. Because of non-invertible one-way property of hash function, it is impossible for an adversary to keep track of all the activities performed by the valid user and thus assures untraceability property. In this scheme, the random numbers and shared secret keys are not stored on the memory. Furthermore, new and distinct session keys are generated using fresh random numbers in every session and hence it ensures the forward secrecy.
- In [39], instead of the original-identity 'IDi', the pseudo-identity 'PIDi' is used and this identity is updated after each communication. Furthermore, one-way cryptographic hash function is used to ensure user anonymity. Because of the unavailability of the random number, attacker can't produce the secret key and thus provides forward secrecy.
- In [40], according to the author, without the private key it is impossible for the attacker to generate valid signcryption and aggregate signcryption and thus provides mutual authentication. Transmitted data are encrypted using certificateless aggregation and signcryption technique to provide data privacy and integrity. Instead of IoT device's actual identity, a registration serial number is provided by the KGC and thus providing user anonymity.
- In [62], identity privacy of the IoT devices is achieved by using lightweight hash and xor operations. The scheme proposed in this work is developed as an alternative to the elliptic curve integrated encryption scheme of 3GPP 5G. As the scheme works alongside 5G-AKA protocol, most of the security issues are already taken care of. However, it may be noted that the scheme is only designed to achieve identity privacy using lightweight mechanism. Other security issues and challenges continues to remain in the same state and of same computational complexity as in 5G-AKA protocol.
- In [63], a Lightweight Secure Access Authentication (LSAA) protocol based on extended Chebyshev chaotic maps is proposed. The protocol can achieve mutual authentication and strong key agreement between UEs and SNs with robust security protection, including identity privacy protection. The UE encrypts its identity 'ID' with key 'K1' that is shared between the UE and the designated SN. Thus, an adversary cannot obtain the ID of UE; hence, LSAA achieves identity anonymity.

Table 2: Recent proposals for 5G-IoT vis-à-vis the security issues addressed.

Paper	Issues resolved	Issues not considered
Cao et al. [31]	mutual authentication, user anonymity, non-repudiation, Integrity, Data Confidentiality	Consumes a lot of computational cost
Yang et al. [32]	Anonymity	Mutual authentication is not considered
Ni et al. [34]	Anonymity, Privacy preserving, Authentication	Issues like forward secrecy and non-repudiation are not considered.
Cao et al. [35]	Data Confidentiality, Authentication, Anonymity, unforgeability	Not designed for roaming services, Consumes a lot of computational and storage cost.
Wang et al. [36]	Authentication, Authorization, Integrity, Reliability	Anonymity, non-repudiation, forward secrecy is not considered.
Jangirala et al. [37]	Confidentiality, User Anonymity and Untraceability, Mutual Authentication and Session Key Establishment, Forward Secrecy	Integrity, non-repudiation is not considered.
Sharma et al. [38]	Confidentiality, Integrity	Consumes a lot of computational and storage cost.
Wu et al. [39]	Authentication, Anonymity, Forward secrecy	Integrity and non-repudiation are not considered.
Zhang et al. [40]	Mutual Authentication, Anonymity, Data privacy, Integrity, Non-repudiation	Consumes a lot of computational and storage cost.
Coudhury et. al. [62]	Identity Privacy, Anonymity	Focus is only on identity privacy and anonymity.
Cao et. Al. [63]	Mutual authentication, Identity Privacy and Forward-Backward Secrecy	Requires setting up of a Centralized Key Generation Centre.

Table 3: Recent proposals for 5G-IoT vis-à-vis the existing security threats.

Paper	Threats taken care of	Security threats.
Cao et al. [31]	replay attacks, man-in-the-middle (MitM) attacks, counterfeiting attack, Anonymity attack, Stolen verifier attack, Eavesdropping attack, Session key leakage attack	DoS attack, Offline guessing attack, brute force attack is not considered
Yang et al. [32]	Anonymity Attack	DoS attack, Man in the middle attack, Eavesdropping attack, brute force attack, replay attack are not considered
Ni et al. [34]	Eavesdropping attacks, man-in-the-middle attacks, Anonymity attack and forgery attacks	DoS attack, Brute force attack, replay attack are not considered
Cao et al. [35]	Quantum attack, Replay attack, Man in the Middle attack, Forgery attack, Denial of Service Attack	Insider attack is not considered.
Wang et al. [36]	Masquerade attack	Several well-known attacks are not discussed/considered.
Jangirala et al. [37]	Reader Impersonation Attack, Tag Impersonation Attack, Replay Attack, Man-in-the-Middle Attack, Ephemeral Secret Leakage (ESL) Attack, Quantum attack, Anonymity attack	Insider attack, Eavesdropping attack, DoS attack are not considered
Sharma et al. [38]	Eavesdropping, Man in the Middle attack, DoS attack,	Replay attack is not considered.
Wu et al. [39]	Privileged insider attack, stolen smart card attack, replay attack, off-line password guessing (opg) attacks	DoS attack, Eavesdropping attack, Man in the middle attack is not considered
Zhang et al. [40]	Replay attack, message Modification attack, Impersonation attacks, Man-in-the-middle attack, Anonymity attack	Dos attack, Eavesdropping attack brute force attack are not considered
Choudhury et. al. [62]	Replay Attack, Man in the Middle Attack	Focus is only on identity privacy and anonymity related attacks.
Cao et. Al. [63]	Replay Attack, Mutual Authentication, Eavesdropping, Man in the Middle Attack,	Man in the Middle attack for compromising Identity Privacy from Visited Serving Network not considered.

However, this scheme requires setting up of a Key Generation Centre (KGC) that everyone trusts and that is responsible for generating the secret keys for the UEs and SNs.

- In [63], according to the author, mutual authentication, session key establishment, identity privacy protection, and perfect forward-backward secrecy are achieved.

A summary of the above discussion is presented in Table 2.

5.2 The Proposals vis-a-vis the Security Threats

To overcome various security threats, present in the literature, researchers have developed different schemes which are as follows and given in Table 3. .

- In [31], elliptic curve Diffie-Hellman (ECDH) key protocol is used to establish the session keys to protect the environment from man-in-the-middle (MitM) attack. Random numbers are used in this scheme to protect the network from replay attack. It is claimed by the author that the scheme is resistant against counterfeiting attack because without having the private key, no adversary can forge the valid aggregate signcryption and the digital signature.
- In [35], it is claimed by the authors that the scheme is resistant against eavesdropping attacks, man-in-the-middle attacks and forgery attacks, because, message exchanged between parties can't be corrupted as the session keys can't be identified by the attackers.
- In [37], because of the addition of random numbers and timestamp value, it is resistant against replay attack. This scheme is resistant against man in the middle attack due to the involvement of secret random numbers.
- In [39], random numbers and timestamps are used in every transmitted message and the timestamp value is validated after each message is received so that adversary can't replay the message without a valid timestamp value and random number and the network is protected from replay attack. It is impossible to guess the identity and password value together which results in protection from off line password guessing attack.
- In [40], random number and digital signature are used to resist the network from replay attack and man in the middle attack. The scheme is also resistant against modification attack and impersonation attack by verifying the network.
- In [62], identity privacy of the IoT devices is achieved by using lightweight hash and xor operations. The scheme proposed in this work is developed as an alternative to the elliptic curve integrated encryption scheme of 3GPP 5G. As the scheme works alongside 5G-AKA protocol, most of the security threats are already taken care of.
- In [63], protection from Man in the Middle (MitM) [64] is not considered.

5.3 The Proposals vis-à-vis their Computational Costs

In an IoT environment, it is of utmost importance that the computation overhead introduced by any protocol is minimum. This is because of the limited processing capability of the IoT devices compared to smart phones. In this section, we analyze the recent proposals in this area with regards to the amount of additional computation introduced by these protocols at the IoT devices. For the analysis, we make the following assumptions (Table 4).

Table 4: Assumptions.

Symbols	Assumptions
m	Number of groups.
n	Number of terminals.
t	Number of authentication vectors sent by the HN.
Tm	Time required for a point multiplication.
Tp	Time required for a pairing operation.
Th	Time required for a hash function operation.
Tl	Time required for a polynomial multiplication.
Tr	Time required for a rotation operation.
Tx	Time required for a XOR operation.
Tsc.en	Time required for a symmetric cipher encryption.
Tsc.dc	Time required for a symmetric cipher decryption.
Tc	Time required for Chebyshev polynomial operation.
Sm	Scaler multiplication.

In Table 5, a comparison, in terms of computational overhead involved in the various schemes present in the literature, is presented. The overheads are calculated by counting the number of cryptographic operations involved at the terminal side and at the network side.

Table 5: Computational overhead.

Proposal	Computational overhead	
	Terminal side	Network side
Cao et al. [31]	5Tm + 2Th	(3n + 1) Th + (4n + 1) Tm
Ni et al. [34]	Sm	2nSm + nTsc.en
Cao et al. [35]	3Th + Tl	nTl + (2m + 1) Th
Jangirala et al. [37]	12Th + 15Tr +25Tx	Not applicable as distributed ledger is used.
Sharma et al. [38]	2Tsc.en + Tsc.dc + 2Tx + 3Th	2Tx + Tsc.en + Tsc.dc
Wu et al. [39]	16Tx + 19Tp + 14Th	32Tx + 47Tp + 27Th
Zhang et al. [40]	4Th + 4Tm	(2n +2) Tm + (2n +1) Th
Choudhury [62]	3Tx + 2Th	514Tx + 512Th
Cao et al. [63]	Tc + 4Th + 2 Tsc.en	8 Tc + 4Th + 2Tsc.en

6. Discussion and Future Research Directions

As already discussed in Section 1, in IoT over 5G cellular network, there are several security challenges; this is due to the resource constraints of the IoT devices. In order to address these security challenges, several schemes and protocols were proposed recently by various researchers. In this paper, a detailed study of these proposals was performed. Such a study

may contribute not only in deriving valuable insights and novel approaches, but also in identifying gaps in current proposals that will help in the process of designing future solutions. While performing the study, security issues and threats that may exist in an IoT environment were also taken into consideration. The computational cost of each of these proposals at the terminal side (IoT device/ UE) and the network side were also calculated and compared with each other.

During the study, it was found that no single scheme, proposed recently, is able to take care of all the security issues and threats. Even though some of the proposals are lightweight in terms of their computation overhead, several important security issues and threats are not considered in these proposals. None of these protocols are able to meet all the security requirements and resource constraints of an IoT device; and to our knowledge, none of them are designed keeping the various possible use cases of IoT in mind. For example: in Choudhury et. al's scheme [62], even though the computation cost at the terminal is just 3Tx + 2Th, it considers authentication of only a single device. However, may schemes like the ones proposed in [31] and [35] considers authentication of the devices in groups, which seems more practical for efficient utilization of bandwidth.

It is observed that all the solutions are proposed as novel solutions with no alignment with the current 5G-AKA; this will make the solutions very difficult to be adopted in a practical scenario, especially after wide scale commercial deployment of 5G cellular network.

It is also observed that none of the proposals suggests a mechanism for registration of the IoT devices with the 5G cellular network. In a practical scenario, an individual will possess several IoT devices in his/her household/ workplace/ business. It will thus be almost impossible for the individual to acquire a USIM or to carry each of the IoT devices to the home network for registration, which is a mechanism that is basic to 5G-AKA. Therefore, there is a need to formulate a mechanism for IoT-5G, through which IoT devices may be registered and deregistered as and when required by the individual from his own place, through his UE, without visiting the HN. It may be noted that the UE, once authenticated, is a trusted party of the HN with whom the HN shares its security credentials.

Future Scope of Research: Based on the study presented in the preceding sections and on the basis of the above discussions, we recommend the following future scope of research in the field of IoT over 5G cellular network.

- There is a need to device lightweight cryptographic solutions for authentication of the IoT devices, over the 5G cellular network, that are low in computational complexity and that takes care of all the known security issues and threats into consideration.
- The solutions have to designed in such a way that they are aligned with the current authentication key agreement protocol used in 5G cellular network (5G-AKA), without requiring much modification, for easy adoption in actual deployments.
- The solutions should allow an individual to register/ deregister an IoT device as an when required through his/her UE. It may be noted that UE is already registered with the HN and it shares security credentials with the HN at the time of acquiring the USIM form the HN.
- The solutions should be such that the UE acts as a gateway and allows the network to authenticate a group of IoT devices in a batch to save bandwidth and communication cost.

7. Conclusion

5G cellular network is set to play a crucial role in future IoT deployments. However, existing security protocols used in 5G cellular network may not be suitable for the resource constrained IoT environment. Therefore, several security schemes and protocols have been proposed by researchers in recent times. In most of the proposals, lightweight cryptographic techniques are used keeping the resource constraints of IoT environment into consideration. However, it is observed in this study that none of them are able to successfully handle all the security issues and threats that may exist in an IoT environment. Moreover, none of the proposals are aligned with 5G-AKA (the AKA protocol adopted in 5G cellular network). This make the proposals difficult to be adopted in a practical scenario. It is also observed that none of the proposals consider the requirement to formulate a simple mechanism for registration and deregistration of the IoT devices with the 5G core network. In a practical scenario it may not be possible to acquire a USIM for every IoT device. Therefore, it may be concluded that the effort to device efficient security schemes for IoT over 5G cellular network is still an active area of research and continued effort in this direction is extremely important for the success of future deployments of IoT over 5G cellular network.

Acknowledgement

The work presented in this paper is sponsored by Cyber Security R&D Division, Ministry of Electronics and Information Technology (MeitY), Govt. of India. Approval number: AAA-22/2/2021-CSRD-MeitY, Dated: 25th February 2021.

References

[1] Ngu, Anne H., et al. "IoT middleware: A survey on issues and enabling technologies." IEEE Internet of Things Journal 4.1: 1-20, 2016.

[2] Dlodlo, Nomusa, and Josephat Kalezhi. "The internet of things in agriculture for sustainable rural development." 2015 international conference on emerging trends in networks and computer communications (ETNCC). IEEE, 2015.

[3] Yuehong, Y. I. N., et al. "The internet of things in healthcare: An overview." Journal of Industrial Information Integration 1: 3-13, 2016.

[4] Guerrero-Ibanez, Juan Antonio, Sherali Zeadally, and Juan Contreras-Castillo. "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies." IEEE Wireless Communications 22.6: 122-128, 2015.

[5] Lutolf, R. "Smart home concept and the integration of energy meters into a home-based system." Seventh international conference on metering apparatus and tariffs for electricity supply 1992. IET, 1992

[6] Zanella, Andrea, et al. "Internet of things for smart cities." IEEE Internet of Things journal 1.1: 22-32, 2014.

[7] Da Xu, Li, Wu He, and Shancang Li. "Internet of things in industries: A survey." IEEE Transactions on industrial informatics 10.4: 2233-2243, 2014.

[8] Akpakwu, Godfrey Anuga, et al. "A survey on 5G networks for the Internet of Things: Communication technologies and challenges." IEEE access 6: 3619-3647, 2017.
[9] Xu, Lina, Rem Collier, and Gregory MP O'Hare. "A survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios." IEEE Internet of Things Journal 4.5: 1229-1249, 2017.
[10] Li, Shancang, Li Da Xu, and Shanshan Zhao. "5G Internet of Things: A survey." Journal of Industrial Information Integration 10: 1-9, 2018.
[11] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7: 1645-1660, 2013.
[12] Ramya, C. Muthu, M. Shanmugaraj, and R. Prabakaran. "Study on ZigBee technology." 2011 3rd International Conference on Electronics Computer Technology. Vol. 6. IEEE, 2011.
[13] Heydon, Robin, and Nick Hunn. "Bluetooth low energy." CSR Presentation, Bluetooth SIG https://www. bluetooth. org/DocMan/handlers/DownloadDoc. Ashx, 2012.
[14] Ostermaier, Benedikt, Matthias Kovatsch, and Silvia Santini. "Connecting things to the web using programmable low-power wifi modules." Proceedings of the Second International Workshop on Web of Things, 2011.
[15] Nandy, Tarak, et al. "Review on security of Internet of Things authentication mechanism." IEEE Access 7: 151054-151089, 2019.
[16] Rahimi, Hamed, Ali Zibaeenejad, and Ali Akbar Safavi. "A novel IoT architecture based on 5G-IoT and next generation technologies." 2018 IEEE 9th Annual Information Technology, Electronics and Cellular Communication Conference (IEMCON). IEEE, 2018.
[17] Mahmoud, Rwan, et al. "Internet of things (IoT) security: Current status, challenges and prospective measures." 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015.
[18] Ahmad, Ijaz, et al. "Overview of 5G security challenges and solutions." IEEE Communications Standards Magazine 2.1: 36-43, 2018.
[19] Choudhury, Hiten. "Enhanced Anonymity: Customized for Roaming and Non-Roaming IoT-Devices in 5G Cellular Network." 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP). IEEE, 2020.
[20] Cao, Jin, et al. "A Survey on Security Aspects for 3GPP 5G Networks." IEEE Communications Surveys & Tutorials 22.1: 170-195, 2019.
[21] Kalra, Sheetal, and Sandeep K. Sood. "Secure authentication scheme for IoT and cloud servers." Pervasive and Cellular Computing 24: 210-223, 2015.
[22] Kumari, Saru, et al. "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers." The Journal of Supercomputing 74.12: 6428-6453, 2018.
[23] Porambage, Pawani, et al. "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications." 2014 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2014.
[24] Parne, Balu L., Shubham Gupta, and Narendra S. Chaudhari. "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network." IEEE Access 6: 3668-3684, 2018.
[25] Gupta, Shubham, Balu L. Parne, and Narendra S. Chaudhari. "SRGH: A secure and robust group-based handover AKA protocol for MTC in LTE-A networks." International Journal of Communication Systems 32.8: e3934, 2019.
[26] hafizul Islama, S. K., et al. "An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for cellular-commerce environments.", 2015.
[27] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15: 2787-2805, 2010.
[28] Tan, Lu, and Neng Wang. "Future internet: The internet of things." 2010 3rd international conference on advanced computer theory and engineering (ICACTE). Vol. 5. IEEE, 2010.
[29] F. Wu, X. Li, L. Xu, A. K. Sangaiah, and J. J. Rodrigues, ``Authentication protocol for distributed cloud computing: An explanation of the security situations for Internet-of-Things-enabled devices," IEEE Consum. Electron. Mag., vol. 7, no. 6, pp. 38_44, Nov. 2018.
[30] Zhao, Kai, and Lina Ge. "A survey on the internet of things security." 2013 Ninth international conference on computational intelligence and security. IEEE, 2013.
[31] Cao, Jin, et al. "Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network." IEEE Internet of Things Journal 6.2: 1561-1575, 2018.
[32] Yang, Hui, et al. "Blockchain-based trusted authentication in cloud radio over fiber network for 5G." 2017 16th International Conference on Optical Communications and Networks (ICOCN). IEEE, 2017.
[33] Al-Aqrabi, Hussain, Phil Lane, and Richard Hill. "Performance Evaluation of Multiparty Authentication in 5G IIoT Environments." Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health. Springer, Singapore, 169-184, 2019.
[34] Ni, Jianbing, Xiaodong Lin, and Xuemin Sherman Shen. "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT." IEEE Journal on Selected Areas in Communications 36.3: 644-657, 2018.
[35] Cao, Jin, et al. "Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System." IEEE Internet of Things Journal 6.6: 9794-9805, 2019.
[36] Wang, Qixu, et al. "LACS: A lightweight label-based access control scheme in IoT-based 5G caching context." IEEE Access 5: 4018-4027, 2017.
[37] Jangirala, Srinivas, Ashok Kumar Das, and Athanasios V. Vasilakos. "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G cellular edge computing environment." IEEE Transactions on Industrial Informatics, 2019.
[38] Sharma, Suraj, et al. "Secure Authentication Protocol for 5G Enabled IoT Network." 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE, 2018.
[39] Wu, Tsu-Yang, et al. "An Authenticated Key Exchange Protocol for Multi-Server Architecture in 5G Networks." IEEE Access 8: 28096-28108, 2020.
[40] Zhang, Yinghui, et al. "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks." IEEE Access 7: 114721-114730, 2019.
[41] Fang, Dongfeng, Yi Qian, and Rose Qingyang Hu. "Security for 5G cellular wireless networks." IEEE Access 6: 4850-4874, 2017.
[42] Zhang, Xiaowei, Andreas Kunz, and Stefan Schröder. "Overview of 5G security in 3GPP." 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2017.
[43] Basin, David, et al. "A formal analysis of 5G authentication." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018.
[44] Heer, Tobias, et al. "Security Challenges in the IP-based Internet of Things." Wireless Personal Communications 61.3: 527-542, 2011.
[45] Suo, Hui, et al. "Security in the internet of things: a review." 2012 international conference on computer science and electronics engineering. Vol. 3. IEEE, 2012.
[46] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." Computer Networks 57.10: 2266-2279, 2013.

[47] Gope, Prosanta, and Tzonelih Hwang. "BSN-Care: A secure IoT-based modern healthcare system using body sensor network." IEEE Sensors Journal 16.5: 1368-1376, 2015.
[48] Robles, Rosslin John, et al. "A review on security in smart home development." International Journal of Advanced Science and Technology 15, 2010.
[49] Eisenbarth, Thomas, et al. "A survey of lightweight-cryptography implementations." IEEE Design & Test of Computers 24.6: 522-533, 2007.
[50] Katagi, Masanobu, and Shiho Moriai. "Lightweight cryptography for the internet of things." Sony Corporation 2008: 7-10, 2008.
[51] Kerry A. McKay, Larry Bassham, Meltem Sönmez Turan, Nicky Mouha, "Report on Lightweight Cryptography", NIST Interagency Report 8114, March, 2017.
[52] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, Jong Hyuk Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions", Journal of Ambient Intelligence and Humanized Computing, Springer-Verlag Berlin Heidelberg, 2017.
[53] Wazid, Mohammad, et al. "Authentication in cloud-driven IoT-based big data environment: Survey and outlook." Journal of Systems Architecture 97: 185-196, 2019.
[54] Nandy, Tarak, et al. "Review on security of Internet of Things authentication mechanism." IEEE Access 7: 151054-151089, 2019.
[55] Katagi, Masanobu, and Shiho Moriai. "Lightweight cryptography for the internet of things." Sony Corporation: 7-10, 2008.
[56] Lee, Jun-Ya, Wei-Cheng Lin, and Yu-Hung Huang. "A lightweight authentication protocol for internet of things." 2014 International Symposium on Next-Generation Electronics (ISNE). IEEE, 2014.
[57] Tewari, Aakanksha, and B. B. Gupta. "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags." The Journal of Supercomputing 73.3: 1085-1102, 2017.
[58] Pilkington, Marc. "Blockchain technology: principles and applications." Research handbook on digital transformations. Edward Elgar Publishing, 2016.
[59] Yli-Huumo, Jesse, et al. "Where is current research on blockchain technology? —a systematic review." PloS one 11.10: e0163477, 2016.
[60] Ahirwal, R. R., & Ahke, M. "Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network". International Journal of Computer Science and Information Technologies, 4(2), 363-368, 2013.
[61] Haakegaard, R., & Lang, J., "The elliptic curve diffie-hellman (ecdh)." Online at https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/Haakegaard+ Lang. pdf, 2015.
[62] Choudhury, Hiten. "HashXor: A lightweight scheme for identity privacy of IoT devices in 5G mobile network." Computer Networks 186: 107753, 2021.
[63] Cao, Jin, et al. "LSAA: A Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks." IEEE Internet of Things Journal 7.6: 5329-5344, 2020.
[64] Almrezeq, Nourah, et al. "Design a secure IoT Architecture using Smart Wireless Networks." International Journal of Communication Networks and Information Security 12.3: 401-410, 2020.