A survey of security and privacy in Next-Generation Internet of Things

Anju Augustin
Rajagiri College of Engineering and Technology

***Abstract*— Recently, IoT (Internet of Things) and Next Generation Networks (5G & 6G) have been an attractive area of research to develop a smart home, smart city environment. These new forms of technology continue to permeate modern-day society and can have significant impacts on business, government, and personal interactions. They promise to deliver significant increases in speed, connectivity, and capacity. Together these technologies are predicted to offer substantial advances in communications. As these technologies grow in prominence, however their security becomes even more crucial. This security needs to consider and accommodate the unique features of these new platforms and build security as a standard. This paper aims to give comprehensive details on existing technologies that are used in IoT networks. They are cloud computing, fog computing, edge computing, SDN (Software Defined Networks), WSN (Wireless Sensor Networks), and CI (Computational Intelligence). These technologies move from centralized cloud computing to decentralized intelligent computing systems. So here makes a comparison of their features and drawbacks from the security and privacy perspectives. And also provide details of different IoT attacks that affects the Next Generation networks and their solutions. This will help to find a better method for the privacy and security of Next Generation- IoT.**

***Keywords*— Next-Generation Networks, IoT, Security and privacy, Cloud. Fog, Edge.**

I. INTRODUCTION

The Next Generation Networks have so many advantages compared with the existing technologies. They are hundred times faster than 4G, larger bandwidth, lower battery consumption, uninterrupted connectivity, remote access and reduced latency. When we combine the Next Generation Networks and IoT, they have multi GBPS data rates, extreme capacity, uniformity, deep awareness, ultra-low latency and security. Also it has so many applications like Smart cities, Smart driving cars, Smart watches, Patients surveillance etc.

The risk of security threats and challenges are also increasing rapidly with the drastic increase in the web of the technology. Not only the technology but also threats are getting very smarter. Protecting the security and privacy have become the primary concerns in this new telecommunication networks. So the security associated with next generation technologies has considered as one of the key requirements. For that primarily consider about different techniques that are used in current IoT networks, then find their advantages and security drawbacks. It is very helpful for selecting more suitable solution for Next-generation networks. Secondly, to analyse different attacks that affect the Next-Generation networks. This analysis leads to find better solutions for these attacks. This will help to make Next-Generation IoT networks efficiently and effectively.

II. RELATED WORKS

There are various surveys on existing networks and IoT security. Sabrina *et al* [1] summarized various security methods used in IoT. They are integrity, confidentiality and non-repudiation integrating Elliptic Curve Cryptography (ECC), Quantum Cryptography, LoRaWAN, Identity-Based Encryption (IBE) mechanisms, RFID authentication and methods of three-factor authentication. For Key management, standard Diffie-Hellman based key exchange and for Intrusion detection-A neural network model are used. The advantages of these methods are, it has the potential to achieve confidentiality, integrity, availability and non-repudiation. A solution based on the integration of ECC and Identity-Based Encryption mechanisms is proposed in order to avoid the non-repudiation of the messages exchanged in device-to-device .2D communications, during the discovery and phases of transmission. In LoRaWAN, mutual authentication method is used, they provide integrity protection, and confidentiality. Data packets, transported over the network, are encrypted and integrity protected, this achieve end-to-end security. Three factor Authentication-The strength of authentication systems is largely determined by the

number of factors incorporated into the system. RFID method automates data collection and reduces human effort and error. The disadvantages are for ECC it's complicated and tricky to implement securely. LoRaWAN is not good for large data payloads and not an ideal candidate for real time applications. Increased log in time, complex deployment and integration. RFID technology is harder to understand and can be less reliable. Rabia *et al*[2] explained novel networking concepts such as Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge Computing (MEC).

The SDN concept helps to centralize the network control. That means network control of SDN based network are placed in a logically centralized controller. For the control functions it can offer an abstract of the underlying network infrastructure and business application layer. A novel approach to create, deploy and manage networking services is proposed by NFV. The aim of this concept is to decouple the network functions from proprietary hardware in order to run them as software instances. On demand scalability for the networks can be achieved by Cloud computing and MEC.

TABLE I Literature Survey

Sl No	Title of the Paper	Citation	Methods Used	Published in	Advantages	Disadvantages
1	5G in the internet of things era: An overview on security and privacy challenges	Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini - Elsevier B.V. - 2020	Integrity, confidentiality and non-repudiation-integrating Elliptic Curve Cryptography (ECC) and Quantum Cryptography, Identity-Based Encryption (IBE) mechanisms, LoRaWAN. Authentication and access control-, RFID authentication, and three-factor authentication, Key management- standard Diffie-Hellman based key exchange Intrusion detection-A neural network model	2020	-It has the potential to achieve confidentiality, integrity, availability and non-repudiation -A solution based on the integration of ECC and Identity-Based Encryption mechanisms is proposed inorder to avoid the non-repudiation of the messages exchanged in different devices ,2D communications, during the discovery and transmission. - In LoRaWAN mutual authentication, integrity protection, and confidentiality. - Data packets, transported over the core network, are both encrypted and integrity is protected, thus achieving end-to-end security. -Three factor Authentication-The strength of authentication systems are largely determined by the number of factors incorporated into the system. - RFID- RFID technology helps to automates the data collection and it reduces human effort and chances of error. -The input is stored in its own networks instead of a database, hence the loss of data does not affect its working. -The input is stored in its own networks instead of a database, hence the loss of data does not affect its working.	-ECC is complicated and tricky to implement securely. -LoRaWAN is- not good for large data payloads. -Not ideal candidate for real time applications. -Increased log in time, Complex deployment and integration -RFID technology is harder to understand. -It can be less reliable
2	Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions.	Rabia Khan, Student Member, IEEE, Pardeep Kumar Member, IEEE, Dushantha Nalin K. Jayakody, Senior Member, IEEE and Madhusanka Liyanage, Member, IEEE 2019	Novel networking concepts such as Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge Computing (MEC)	2019	-The SDN concept centralizes the control and data planes of networking device. It is a logically centralized controller. It can offer an abstract of the underlying network infrastructure for the control functions and business application layer. -NFV proposes a novel approach to create, deploy and manage networking services. This concept helps to run them as software instances. -Cloud computing and Mobile Edge Computing will enable on demand scalability for the networks.	

3	A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things.	Sooyeon shin , (member, ieee), and Taekyoung Kwon , (member, ieee)- IEEE-2020	Fuzzy extractor- extracts biometric information as a uniformly random string with an error tolerance limit t from a biometric template. Elliptic curve cryptography-The Elliptic Curve Discrete Logarithm and ECC based anonymous authentication, authorization and key agreement scheme.	2020	-This increase connectivity and provide convenient service. -It remedies security vulnerabilities based on the system architecture in WSNs for 5G-integrated IoT. -ECC scheme is split into five phases: (1) setup; (2) user registration; (3) authentication, authorization, and key agreement (AAK); (4) password and biometrics update; and (5) access privilege update. -ECC provides three-factor user authentication and overcomes the security weaknesses, not only satisfies various security features such as authorization, but also withstands all known attacks.	- Fuzzy extractor increases the number of attack. -In the heterogeneous 5G-IoT environment, the increasing number of IoT devices increases vulnerability for various spoofing attacks.
4	Anonymous Communications for Secure Anonymous Communications for Secure Device to Device Aided Fog Computing	Prosanta Gope, Jemin Lee, Ruei Hau Hsu, and Tony Q.S. Quek, IEEE consumer electronics magazine- 2019	D2D communication aided fog computing model - CCS involved (conventional) authentication scenario - ED aided authentication scenario -NAD aided authentication scenario	2019	-It can be used to support efficient communication and security of the EDs (Edge Devices). -During the authentication processes, used lightweight cryptographic primitives, like one-way hash function and exclusive-or operations, which makes fog-computing model more feasible for resource-limited IoT devices. -They reduce communication latency and also offload the overhead, we estimated the latency in three authentication protocols (CCS-Auth, ED-Auth, and NADAuth) for secure communications in the proposed security architecture.	-Encryption algorithms and security policies make it more difficult for devices to exchange data. Any mistakes in security algorithms will leads to an exposure of sensitive data to the hackers.
5	Fog Computing Architectures, Privacy and Security Solutions	Wasswa Shafik,Seyed Akbar Mostafavi- Journal of Communications Technology, Electronics and Computer Science- 2019	Hybrid Cloud Computing model.	2019	-With this model, the flexibility of storing sensitive data securely in a private cloud while storing public data in a public cloud. -This provides reduced costs like establishing, and running a data centre. -It provides flexibility, mobility, scalability. -No need for a backup plan.	-Security is the one of the main problem in the cloud. Mainly if handle grouped data and customer information. -Consistency is the another issue which leads requirement of private cloud to protect private data
6	Intelligence Enabled Cybersecurity for the Internet of Things	Shanshan Zhao , Shancang Li , Senior Member, IEEE, Lianyong Qi , and Li Da Xu, Fellow,IEEE transactions on emerging topics in computational intelligence- 2020	Fuzzy logic, neural networks, evolutionary computation, learning theory. Technologies in CI enabled cybersecurity CI based algorithms includes biologically inspired algorithms and decision making algorithms. CI Enabled Malware and Threats Detection for IoT- by providing detailed attributes or behaviors to analyze false positives or	2020	-The CI techniques promising to help IoT systems to detect security patterns from data and learn them to adjust their behaviour to avoid potential cyber threats. -Self-training CI algorithms (such as deep learning) can be used to labelled to identify insider threats that human being unable to differentiate from normal behaviour. -Accessing patterns within the data, CI classifiers are able to effectively label data as malicious, thus increasing the level of security and the ability of administrators to more effectively monitor the complex IoT systems. -An anomaly detection aims to offer key security functionalities such as monitoring,	-The CI enabled techniques brings threats to cyber security. It is reported that the CI techniques are used to develop techniques for unlocking doors and transferring money using devices. -Attackers use CI techniques to develop powerful attacking tools, like malware, ransomwares, CI-

			negatives and improve model prediction accuracy		detecting, analysing, and responding to unauthorized traffic.	enabled attack kits, etc.
7	A Comprehensive Survey on Internet of Things (IoT) Towards 5G Wireless Systems.	Lalit Chettri 1, Rabindranath Bera-IEEE Internet of Things journal-2019	Enhanced mobile broadband (eMBB), enhanced machine type communication (eMTC) and critical communications (URLLC). The Massive MTC Smart sensors in sensor layer	2019	-These technologies will enable machine to machine (M2M), device to device (D2D) and device to everything (D2E) communication, internet of things (IoT) and internet of vehicles (IoV) -The name implies more connected objects for example, e-health services, City/village, e-Farm, intelligent transportation system (ITS), whose end-to-end cost must be sufficiently low to make cost effective ensuring secured communication. -The smart sensors are capable of two-way communication between the sensors and network layers and make their communication and make the decisions. Smart Communication between Devices, Sensors, and Network Protocols -Flexible Connection and low cost and power.	

SOOYEON *et al*[3] have discussed the FUZZY EXTRACTOR, that can extract biometric information from a biometric template, as a uniformly random string with an error tolerance limit t. And ELLIPTIC CURVE CRYPTOGRAPHY it uses the Elliptic Curve Discrete Logarithm ECC-based anonymous authentication, authorization and key agreement scheme. The advantages of these methods were explained in the table.

Prosanta Gope *et al*[4] focus mainly on D2D communication aided fog computing model. It includes CCS involved (conventional) authentication scenario, ED aided authentication scenario and NAD aided authentication scenario. It can be used to support efficient communication and security of the EDs(Edge Devices).

Wasswa Shafik *et al*[5] have surveyed hybrid Cloud Computing model in IoT. With this model, the flexibility of storing sensitive data securely in a private cloud while storing public data in a public cloud. This provides reduced costs like establishing, and running a data Centre by no need of a backup plan, data security, and improved collaboration among others in the merits. The disadvantages of these model is that security is stress in the cloud, mainly if handle grouped data or customer information. Consistency in the cloud may become a problem. So, it may require the creation of private cloud to protect private data.

Shanshan Zhao *et al*[6] have discussed fuzzy logic, neural networks, evolutionary computation, learning theory. Technologies in CI enabled cybersecurity: First one CI based algorithms, it includes biologically inspired algorithm, decision making algorithms. Second is CI Enabled Malware and Threats Detection for IoT.

Lalit Chettri *et al*[7] summarized that 5G new radio technologies feature in enhanced mobile broadband (eMBB), enhanced machine type communication (eMTC), critical communications (URLLC) and Augmented Reality(AR) in 5g iot. These technologies will help machine to machine (M2M), device to device (D2D) and device to everything (D2E) communication, internet of things (IoT) and internet of vehicles (IoV). The main role of AR in 5G IoT is to enhance human perception about the system scenario and environment by additional computer generated information through PCs, Laptops, Smartphone's, Tablets, Projectors etc. The information generate by AR are in the form of images, videos, texts, 3D models etc. By these resources, the user is able to get the information about the communication within IoT environment. AR can be feasible in IoT applications such as smart homes, smart factories, smart offices, medical surgeries (telemedicine), military, logistics etc.

The literature survey found that existing IoT networks have so many advantages in security and privacy. Also, they have some problems. These methods can't be used directly for the Next Generation IoT because they have advanced features and architecture. So it needs new security mechanisms or existing methods with modifications. For this, need a deeper analysis of the security features of different techniques and computing methods that are used in existing IoT.

III. DIFFERENT IOT NETWORKING MODELS:

IoT uses smart solutions with embedded intelligence, connectivity, and processing capabilities for devices that rely on real-time and non-real-time analysis of information. These systems are moving from centralized cloud computing solutions towards distributed intelligent computing systems. Cloud computing solutions are perfect for non-real-time applications that require high data rate, huge amount of storage, and less security. Distributed solutions such as fog computing, edge computing, WSN, etc. introduce computations at the edge of the network and are useful for real-time applications. The collection, storage, and processing of data at the edge of the network increase the privacy for the user data.

1.Cloud Computing
2 Fog Computing
3 Edge Computing
4 SDN
5 WSN
6 Computational Intelligence

1.Cloud Computing

Cloud computing is a centralized two-tier network architecture, front tier represents mobile network and the back tier encircles cloud devices. Data centres or baseband units stores and process large amount of data from end devices and thus form the backbone of cloud computing model. There are three types of Clouds, Private cloud, Public cloud and Hybrid cloud. Private cloud is a single environment used by organizations that does not share their resources with others. Public cloud provides public or free access for anyone. Hybrid cloud combines the features of these two.

TABLE II Analysis of Cloud computing security

Advantages	Disadvantages
• Providing enough energy resources, cost reduction and supporting multiple platforms. • Efficient recovery. • Openness-Get to your data wherever, at whatever point. • No material required-Sinc everything will be encouraged within cloud.	• low latency and backhaul bandwidth limitations are serious issues of cloud computing. • Delay in communication between end IoT devices (EIDs) and cloud . • Cloud computing architecture requires complicated software to interconnect all devices using cloud servers. • Economic Impact of a DoS Attack. • Insufficient Security of Internet Channels-Interaction with the cloud occurs through Internet channels, which, without proper protection. • Risk of data confidentiality.

2.Fog Computing

Fog computing extends the concept of cloud computing making it ideal for internet of things (IoT) and other applications which require real-time interactions. It is a decentralized computing infrastructure in which data, compute, storage and applications are located between the data source and the cloud. It bringing intelligence and processing closer to where the data is created.

TABLE III-Analysis of Fog computing security

Advantages	Disadvantages
• Fog computing is more suitable for IoT applications. • Content delivery, mobile big data analytics, and augmented reality are three core scenarios which will benefit from fog the most. • D2D aided communication. • Fog computing brings opportunities to provide quality and prompt services in health. • Privacy-Any sensitive data of the user can be analyzed locally instead of sending them to a centralized cloud infrastructure. • The operations take place at various end points in a complex distributed environment. This makes it easier to identify potential threats before it effects the whole network. • Low latency and dynamic per-user optimization, among others.	• Encryption algorithms and security policies make it more difficult for arbitrary devices to exchange data. Any mistakes in security algorithms lead to exposure of data to the hackers. Other security issues are IP address spoofing, man in the middle attacks, wireless network security etc. • To achieve high data consistency in the fog computing is challenging and requires more efforts. • Trust and authentication are major concerns. • Hackers can easily impose fake IP address in them gaining access to the respective fog node. • Increase the risk of corrupted files infiltrating the main data stream infecting both the device and the company. This makes them vulnerable to Man-in-the-middle attacks. • Service offered by a fog computing is of large scale. The fog computing is comprised of end users, internet service providers and cloud providers. This can often rise trust and authentication issues in the fog.

3.Edge Computing

Edge computing is a networking methodology focused on bringing computing close to the source of data in order to reduce latency and bandwidth. In simpler terms, edge computing means running fewer processes in the cloud and moving the processes to local places, such as on an IoT device, a user's computer or an edge server. The edge computing model consist of edge devices, edge nodes they are like routers and cloud infrastructures.

TABLE IV-Analysis of Edge computing security

Advantages	Disadvantages
• One of the benefits of edge computing is a reduction in latency. • Edge computing distributes processing, storage, and applications across a wide range of devices and data centers, which makes it difficult for any single disruption to take down the network. • Sometimes the edge computing does not require a network connection at all. Even if the hackers manage to infiltrate the cloud, not all the information of the user are at risk.	• Data processing takes place at the outside edge of the network there are often risks of identity theft and cyber security breaches. • Whenever a new IoT device is added here, it will increase the opportunity for the attackers to infiltrate the device . • Edge computing only process and analyze partial sets of information. The rest of the data are just discarded.

• Edge computing reduces the amount of data that has to travel over a network, which is an obvious bonus from a security perspective. • Providing manufacturers of smart products make securing that local data a key priority. • With edge computing, there's an opportunity for enhanced security management with the hardware, software and security packaged together. • Significant bandwidth savings because of edge computing.	• Edge computing does take a considerably higher storage space on your device. • Implementing an edge infrastructure can be costly and complex • Higher maintenance cost than a centralized infrastructure.

4. SDN (Software Defined Networks)

Software-Defined Networking (SDN) is a network architecture in which the network is to be intelligently and centrally controlled, or 'programmed,' using various software applications. This helps operators to manage the entire network, regardless of the underlying network technology, consistently and holistically. SDN architecture contains three layers' application, control and infrastructure layer. The SDN controller is the most important component they provide centralized controlling of the system. The features are agile, directly programmable, and centrally managed.

TABLE V Analysis of SDN security

Advantages	Disadvantages
• Centralized intelligence. • In SDN network and security policies are maintained and managed in the controller, it becomes relatively less difficult to get the policy evenly distributed throughout the network. • To sidestep proprietary controls and develop tools that will simply security across the network. • More transparent for analysis and event response. • Security becomes scalable. • Greater visibility throughout the network. • Can manage the network via the SDN controller, without the need to access the individual networking devices.	• Hypervisor vulnerabilities. • Vulnerable to denial-of-service attacks. • Attackers only have to access one node i n your network — the SDN controller - to have control of your entire network s ecurity.

5. WSN (Wireless Sensor Networks)

Wireless sensor networks consist of hundreds small devices each with sensing, processing, and communication capabilities to monitor the real-world environment. It has a base station which acts like an interface between users and the network. It is an infrastructure less network model and sensors are deployed in an ad-hoc manner. It helps to monitor physical or environmental conditions.

TABLE VI Analysis of WSN security

Advantages	Disadvantages
• SDN networks give operators more power, control, flexibility and visibility. • Wireless sensor networks are used in those harsh and hostile environments where wired networks can't be deployed. For example in a forest. • The wireless sensor networks are scalable • That is why they are actively being used in applications such as Structural Health Monitoring . • Can easily be deployed without any hustle	• Limited computation and communication resources. • Less secure because hackers can enter the access point and obtain all the information • Lower speed as compared to a wired network. • More complicated to configure compared to a wired network.

6. Computational Intelligence(CI)

CI plays a major role in developing successful intelligent systems, including games and cognitive developmental systems. It is the ability of a computer to learn a specific task from given data or experimental observation. The methods used here is more close to human's way of reasoning. Five main principles of CI are Neural networks, Fuzzy logic, Evolutionary computation, Learning theory, Probabilistic methods.

TABLE VII
Analysis of CI security

Advantages	Disadvantages
➢The CI techniques are promising to help IoT systems to detect security patterns from data and learn to adjust their behavior to avoid potential cyber threats. ➢CI techniques are adopted to improve cybersecurity, including learning to detect suspicious behaviors, stopping cyberattacks, etc. ➢Can identify and detect malicious piece of intelligent code and getting it out of the IoT systems in a timely and automated way.	➢ CI could be used by attackers to develop more powerful attack tools, including malware, ransomwares, CI-enabled attack kits, and more.

TABLE VIII
NEXT-G IoT ATTACKS

IV. DIFFERENET NEXT-GENERATION IOT ATTACKS

The Next-Generation networks enabled IoT used to sense, collect, store, process, transmit, create, manage and analyse data. The combination of this new technology, IoT and distributed security brings new challenges in Next Generation IoT networks. Each of the IoT techniques have here own security merits and demerits. So combining one or more techniques gives more security and privacy, like Intelligent Edge. This analysis also considering different attacks that affect the Next-Generation IoT. This will help to implement more reliable and effective Next-Generation IoT networks in the future. The threats and attacks have

been on the increase in both number and complexity. The threats cause physical damage, unauthorized access, theft, or loss of data.

Slno	Citation	Attack	Target	Weaknesses	Techniques	Solutions
1	Yuchong Li ,Qinghui Liu - A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments-Elsevier 2021	DDoS	IoT devices	-Reduction in network capacity. -Disable the network	-IP enable status contributes to a pool thing. -Distributed attack utilized and auto shut IoT system.	-Develop a Denial of Service Response Plan. -Secure Network Infrastructure. -Maintain Strong Network Architecture. -Leverage the Cloud.
2	Mukrimah Nawir, Amiza Amir, Naimah Yaakob, Ong Bi Lynn-Internet of Things (IoT): Taxonomy of Security Attacks-IEEE 2019	Wormholes	Location of the packets	-Problematic in checking the routing information	-Record the packets at one location then tunnel it to a different location.	-Select a Leader from MANETS and mitigate attack by using selection algorithm. -The best leader's work is to find the path with the vulnerability that is a path with wormhole tunnel.
3	Mukrimah Nawir, Amiza Amir, Naimah Yaakob, Ong Bi Lynn-Internet of Things (IoT): Taxonomy of Security Attacks-IEEE 2019	Spoofed, alter or replayed Routing information	Routing information and Detectable IoT devices	-High end to low end latency -Routes sources might be extended or shorten.	-First spoofer only listens and then acts when the transmitter stops sending a signal, then unreliable signal send.	-Monitoring networks for a typical activity -Deploying packet filtering -robust verification -Authenticating all IP addresses -Using a network attack blocker
4	Yuchong Li ,Qinghui Liu - A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments-Elsevier 2021	Sybil	Integrity of data security and resource utilization.	-Launch threat to routing protocol. -Costly network.	-It propagates malware to a website. -The adversary is impersonate the normal users.	-Identity validation. -Social trust graphs. -Economic costs. -Application-specific defences is a good method.
5	Mukrimah Nawir, Amiza Amir, Naimah Yaakob, Ong Bi Lynn-Internet of Things (IoT): Taxonomy of Security Attacks-IEEE 2019	SQL Injection	Database	-Degradation of system integrity	-Invalid data injection.	- Use of Prepared Statements (with Parameterized Queries) - Use of Stored Procedures. - Allow-list Input Validation. - Escaping All User Supplied Input.
6	Aufner, P. The IoT security gap-Springer-2019	Eavesdropping	System data	-Reduce data collection and affect data in motion	Unauthorized interception of system data	-Using a personal firewall -Keeping antivirus software updated -Using a virtual private network (VPN) -Strong authentication and encryption techniques
7	Yuchong Li ,Qinghui Liu - A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments-Elsevier 2021	Malware	System data	-Interfere with proper system operation	-Malicious code injection to hostage target data using crypto virology techniques	- Change in default passwords/always change default passwords. -Remove devices with telnet backdoors. -Never expose a device directly to the internet. -Run port scans on all machines. -Using signatures to block known malicious code.
8	Zeinab Bakhshi, Ali Balador and Jawad Mustafa-	Brute Force	Database	-Repetitive attempts to infiltrate the	-Use exhaustion methods to do trial and error to	-Use strong passwords - Enable two factor authentication.

	IEEE Wireless Communications and Networking Conference-2018			system by means of exhaustive combinations of possible credentials	find out a legible access or decode encrypted data.	-Restrict number of failed attempts of data access. -Restrict access from other IPs. -Enable CAPTCHA.

1.DDoS attack

Compared to conventional DDoS attacks, IoT DDoS attacks are very harder to be defended against. Because IoT devices have limited storage and computational resources. Next-generation IoT's are characterized by the usage of smart solutions with embedded intelligence at the edge that relies on high connectivity, real-time analysis of information, and processing capabilities for edge devices. Also, it's very harder to find security threats. In DDoS attacks attacker attempts to obstruct or stop legitimate users from accessing specific network services or resources by distributed attack sources. An attacker can create a botnet by compromising vulnerable internet connected devices and launches attacks by controlling the botnets through a control server; as a consequence, the victim receives

massive source-varied attack traces that disrupting its normal activities. Different types of IoT DDoS attacks are:

I. Flooding-based Attacks - This type of attacks aims to exhaust a victim's resources or the network bandwidth based on massive disguised network packets.

1. Naive Flooding Attacks - The malicious packets employed for this attacks are always composed of a large number of repetitive communication requests, which fill the victim's buffer. When the buffer is full, the victim cannot accept new messages.

2. Protocol Exploitation Attacks – These attacks are triggered by protocol features and implementation bugs. Attackers can exploit specific features of the network and run out of resources.

3. Reflection-based and Amplification - based Attacks. In Reflection based attacks, attackers send malicious request packets to a server. The server is unable to distinguish the spoofed packets from legitimate ones. Then massive response packets are then directed to the victim from the server. In Amplification-based attack attackers aim to fraud the server to generate a high volume of response packets to a victim with limited requests.

II. Slow Request/Response Attacks - Here attackers hold the communication channel and exhaust the resources of a victim by spoofing high-workload of requests or responses.

2.Wormholes Wormhole attacks extremely hard to find because it is an internal attack which listens to the network activities without changing it.

Effects of this attack:

- Selectively drop data packets
- Routing disruption
- Bypasses large amount of network traffic
- Modifying packets, changing the sequence of packets, etc.
- By analyzing the collected data, the attacker can perform other more aggressive attacks like man-in-the-middle attacks, cipher breaking etc.

3. Spoofed, Alter, Replay Routing Information

It is a mutual direct attack. It targets on routing information. That means they attack where the data exchange between nodes occurs. Spoofing attacks are created by creating a routing loop, generating a false error message and many more techniques. In the beginning attack, the spoofer does not transmit any signal, but they listen to the proper transmitter. When the legitimate transmitter stops sending signal to the legitimate receiver, spoofer starts sending the unreliable signal.

4. Sybil attack

Sybil attack is a single node attack that has multiple identities. That means the attacker can be in more than one location at a time. It will degrade the data integrity, security and resource utilization.

This attacks are mainly launched by propagating malware to a website to steal the information. Comprehensively, it is like a masquerade, that means it looks like ordinary users but it is not. It is very important to have a security defence to maintain the IoT system so that it can keep working correctly. Two types of Sybil attacks: Direct and indirect.

- In direct attack, the honest(trusted) nodes are influenced directly by the Sybil nodes.
- In indirect attack, the honest nodes are attacked by a node and that node communicates directly with the Sybil nodes. This middle node is compromised as malicious influence of Sybil nodes.

5.SQL injection

Here a malicious SQL code injected into the database that was not the intended one to access. It gives hacker's to access the underlying database and attacker can delete, copy or modify the contents of the database and can also modify cookies to poison application's database query. The main solutions for this attack are input validation and use of parameterized queries. The application should never use input directly, must sanitize all inputs. In parameterized queries the *SQL* statements are sent to and parsed by the database server separately from any parameters.

6.Eavesdropping attack

This attack occurs when hackers access, delete interpret, or modifies data that transmitted between devices. This attack also known as snooping or sniffing. It relies on unsecured network communication to access data. Two types of eavesdropping, passive and active. In passive eavesdropping hacker only listens to the data that are passing through the network. In active attack attacker disguise themselves, read or steal data.

7.Malware

Malware means it is a malicious software or code that designed to gain access and damage computer or device. These devices are always connected to the internet and have lack of security. By Malware attack, attackers can hit thousands of devices and once the attacker gets access to these devices it launches DDoS attack on victim.

8. Brute Force attack

Brute force attack means attackers trying to attack websites or servers by a long list of passwords. They assume that anyone combination become correct. The main goals of these type attack are to steal personal information, information phishing, credential stuffing etc. We can recognize this attack by looking for number of failed attempts to login from same IP or an increase in load on server.

V. CONCLUSIONS

The Next-generation networks with IoT will conquer the technology world in the future. It has lots of new technologies, such as 5G, advanced robotics, etc. As technologies grow in prominence, the security problem will also increase. So need to analyze and study about the existing technologies that are used in the IoT networks and different attacks that affect them. This paper surveys and examines the literature on the existing technologies and attacks on IoT networks. By this analysis, it was found that each method have their own advantages and disadvantages.

Cloud computing provides high storage space, but the attacker can easily access its centralized feature. Fog computing have low latency, but extra resources are needed to implement them. Edge computing provides low latency and extra security, but it causes higher overhead on networks. SDN efficiently control networks using software, but this centralized controller easy susceptible to attacks. WSNs are lightweight and ad-hoc in nature, but in critical area such as military applications sometimes it undergoes security vulnerabilities. CI is one of the efficient and emerging technology that provides artificial intelligence to the networks. So they can easily identify and secure themselves from security and privacy issues. But sometimes it used as a tool for attacks. In the future, the most important issues faced by Next-Generation IoT networks are security and privacy. So, this paper attempts to find possible solutions for these attacks. This would help to develop more reliable and secure next-generation IoT networks.

REFERENCES

[1] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini - "5G In The internet of things era:An Overview On Security and Privacy challenges."- 2020 Elsevier B.V.

[2] Rabia Khan, Student Member, IEEE, Pardeep Kumar Member, IEEE, Dushantha Nalin K. Jayakody, Senior Member, IEEE and Madhusanka Liyanage, Member, IEEE-" A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions"-journal of IEEE communications surveys and tutorials, 2019.

[3] Sooyeon Shin, (Member, IEEE), and Taekyoung Kwon, (Member, IEEE) "A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things"- IEEE Access, -, 2020

[4] Prosanta Gope, Jemin Lee, Ruei-Hau Hsu, and Tony Q.S. Quek "Anonymous Communications for Secure Device-to-Device-Aided Fog Computing "-IEEE May 2019.

[5] Wasswa Shafik, Seyed Akbar Mostafavi, "Fog ComputingArchitectures, Privacy and Security Solutions" - Journal of Communications Technology, Electronics and Computer Science, Issue 24, 2019

[6] Shanshan Zhao, Shancang Li, Senior Member, IEEE, Lianyong Qi, and Li Da Xu, Fellow, IEEE" Computational Intelligence Enabled Cybersecurity for the Internet of Things"-2471-285X © 2019 IEEE.

[7] Lalit Chettri, Rabindranath," A Comprehensive Survey on Internet of Things (IoT) Towards 5G Wireless Systems"-IEEE internet of things journal-2019.

[8] Kinza shafique , Bilal a. Khawaja, (senior member, ieee), Farah sabir, Sameer Gazi , (member, ieee), and Muhammad mustaqim - "Internet of Things (IoT) for Next-Generation Smart Systems:MA Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios"-IEEE Access-2020.

[9] Blesson Varghese, Nan Wang, Sakil Barbhuiya, Peter Kilpatrick and Dimitrios S. Nikolopoulos-" Challenges and Opportunities in Edge Computing"- 2016 IEEE International Conference on Smart Cloud.

[10] Alejandro Molina Zarca∗, Jorge Bernal Bernabe∗, Antonio Skarmeta∗, Jose M. Alcaraz Calero-"Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks "-IEEE journal on selected areas in communications-2020

[11] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, Ong Bi Lynn- Internet of Things (IoT): Taxonomy of Security Attacks.

[12] Hamed Rahimi, Ali Zibaeenejad, Ali Akbar Safavi- A Novel IoT Architecture based on 5G-IoT and Next
Generation Technologies-2019

[13] Zeinab Bakhshi, Ali Balador and Jawad Mustafa-IEEE Wireless Communications and Networking Conference-2018.

[14] C. Vijayakumaran B. Muthusenthil, B. Manickavasagam-A reliable next generation cyber security architecture for industrial internet of things environment-2020

[15] Gabriel Neagu*, Marilena Ianculescu, Adriana Alexandru, Vladimir Florian, Constanța Zoie Rădulescu - Next generation IoT and its influence on decision-making. An illustrative case study- ELSEVIER-2019

[16] "Size of the internet of things (iot) market worldwide from 2017 to 2025," https://www.statista.com/statistics/976313/global-iotmarket-size/l, 2018.

[17] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis et al., "Understanding the mirai botnet," in 26th {USENIX} Security Symposium ({USENIX} Security 17), 2017, pp. 1093–1110.

[18] "Inside the infamous mirai iot botnet: A retrospective analysis," https://blog.cloudflare.com/inside-mirai-the-infamous-iotbotnet-a-retrospective-analysis/, 2017.

[19] "The iot rundown for 2020: Stats, risks, and solutions," https://securitytoday.com/Articles/2020/01/13/The-IoTRundown-for-2020.aspx?Page=2, 2020.

[20] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, - IEEE Commun. Mag., vol. 53, no. 4, pp. -2015

[21] Z. Ning, X. Kong, F. Xia, W. Hou, and X. Wang, "Green and Sustainable Cloud of Things: Enabling Collaborative Edge Computing," IEEE Communications Magazine, vol. 57, no. 1, pp. 72–78, Jan. 2019.

[22] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[23] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "Towards a systematic survey of industrial IoT security requirements: research method and quantitative analysis," in Proceedings of the Workshop on Fog Computing and the IoT, 2019, pp. 56–63

[24] S. Deep, X. Zheng, and L. Hamey, "A survey of security and privacy issues in the Internet of

Things from the layered context," arXiv preprint arXiv:1903.00846, 2019

[25] G. Choudhary and V. Sharma, "A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks," in 5G Enabled Secure Wireless Networks, Springer, 2019, pp. 69–102

[26] R. Kumar, P. Kumar, and V. Singhal, "A Survey: Review of Cloud IoT Security Techniques, Issues and Challenges," Issues and Challenges (March 12, 2019), 2019.

[27] . Yousefpour et al., "All one needs to know about fog computing and related edge computing paradigms: a complete survey," Journal of Systems Architecture, 2019.

[28] 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.

[29] S. Kitanov, B. Popovski, and T. Janevski, "Quality Evaluation of Cloud and Fog Computing Services in 5G Networks," in Enabling Technologies and Architectures for Next-Generation Networking Capabilities. IGI Global, 2019, pp. 1–36.

[30] . Han, S. Wong, C. Mannweiler, M. R. Crippa, and H. D. Schotten, "Context-Awareness Enhances 5G Multi-Access Edge Computing Reliability," IEEE Access, vol. 7, pp. 21 290–21 299, 2019

[31] ommunications, 2019. [9] S. Sarraf, "5G Emerging Technology and Affected Industries: Quick Survey," American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), vol. 55, no. 1, pp. 75–82, 2019.

[32] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A Survey," Journal of Industrial Information Integration, 2018

[33] R. Ahmed, A. K. Malviya, M. J. Kaur, and V. P. Mishra, "Comprehensive Survey of Key Technologies Enabling 5G-IoT," Available at SSRN 3351007, 2019.

[34] R. P. Jover, "The current state of affairs in 5g security and the main remaining security challenges," arXiv preprint arXiv:1904.08394, 2019

[35] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G Security: Analysis of Threats and Solutions," in Standards for Communications and Networking (CSCN), 2017 IEEE Conference on. IEEE, 2017, pp. 193–199.

[36] S. K. Mohapatra, B. R. Swain, and P. Das, "Comprehensive Survey of Possible Security Issues on 4G Networks," International Journal of Network Security & Its Applications, vol. 7, no. 2, p. 61, 2015.

[37] V. Sharma, I. You, K. Andersson, F. Palmieri, and M. H. Rehmani, "Security, Privacy and Trust for Smart Mobile-Internet of Things (MIoT): A Survey," arXiv preprint arXiv:1903.05362, 2019.

[38] J.-Y. Yu and Y.-G. Kim, "Analysis of IoT Platform Security: A Survey," in 2019 International Conference on Platform Technology and Service (PlatCon). IEEE, 2019, pp. 1–5.

[39] JayasreeSengupta[a], SushmitaRuj[b], SipraDas Bit[a]-A Comprehensive Survey on Attacks, Security Issues and Solutions for IoT and IIoT-ELSEVIER 2020

[40] . Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing. IEEE, 2009, pp. 729–734.

[41] C. She, W. Wen, Z. Lin, and K. Zheng, "Dad-mcnn: Ddos attack detection via multi-channel cnn," Proceedings of the 2019 11th International Conference on Machine Learning and Computing, pp. 484—-488, February. 2019.

[42] C. VijayakumaranB,. MuthusenthilB, Manickavasagam- A reliable next generation cyber security architecture for industrial internet of things environment -IJECE-2020