Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures

Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul, Imran Zualkernan
Department of Computer Science and Engineering
American University of Sharjah, UAE

Abstract

This paper presents a survey and an analysis of the current status and concerns of Internet of things (IoT) security. The IoT framework aspires to connect anyone with anything, anywhere. As opposed to the traditional Internet, in addition to humans, an IoT connects a large number of machines, resource-constrained devices and sensors using heterogeneous wired and wireless networks. An IoT typically has a three conceptual layers consisting of Perception, Network, and Application layers. This paper describes security issues within and across these layers. Many security principles that should be enforced at each layer are also presented. Previous work specific to enforcing security for each IoT layer and corresponding countermeasures are also discussed. Finally, the paper presents future directions for securing the IoT.

1. Introduction

Internet of things (IoT) is a collection of interconnected objects, services, people, and devices that can communicate, share data, and information to achieve common goals in different areas and applications. IoT can be implemented in many different domains including transportation, agriculture, healthcare, energy production and distribution, and many other areas that require things to communicate over the Internet to perform business tasks intelligently without human involvement. Devices participating in IoT typically follow an Identity Management (IM) approach to be identified in a collection of similar and heterogeneous devices. A region in IoT can be defined by an IP address, however within that region each entity has a unique ID by which it is identified.

The purpose of IoT is to transform the way we live today by enabling intelligent devices around us to perform daily tasks and chores with minimal human intervention. Smart homes, smart cities, smart transportation and infrastructure etc. are the terms which are used in relevance to IoT. The concept of IoT has also been adopted in many sci-fi TV shows, cartoons, and movies and though it seems very difficult to accomplish, but it is a fact that many facets of IoT will be realized in the near future.

There are various application domains for IoT, ranging from personal to enterprise environments [1]. The applications in personal and social domains enable the IoT users to interact with their surrounding environment and other human users to maintain and build social relationships. Another application of IoT is in the transportation sector, in which various smart cars, smart roads, and smart traffic signals serve the purpose of safe and convenient transportation facilities. The enterprise and industries domain of IoT encompass the applications used in finance, banking, marketing etc. to enable different inter- and intra-activities in organizations. The last application domain is the service and utility monitoring sector which includes agriculture, breeding, energy management, and recycling operations, etc.

IoT applications have seen rapid development in recent years primarily due to emergence of newer technologies like Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN). RFID enables the tagging or labeling of every single device, so as to serve as the basic identification mechanism in IoT. Due to WSN, each “thing” (e.g., people, devices etc.) becomes a wireless identifiable object that can communicate among the physical, cyber, and digital worlds [1].

The rest of this paper is organized as follows. Section 2 describes the three-layer IoT framework and architecture. In Section 3, security issues corresponding to different security principles and the nature of IoT devices are presented. This section also contains the security issues associated with each layer of the IoT. Section IV discusses recent research works that attempt to address the security issues in IoT by suggesting countermeasures. Section 5 provides the big picture of all the security-related examined work in IoT. Section 6 addresses the future directions that can be taken in light of the current status of IoT security. Finally, the paper is concluded in Section 7.

2. IoT Architecture

In an IoT architecture, each layer is defined by its functions and the devices that are used in the layer. There are different opinions regarding the number of

layers in IoT. However, according to many researchers [2-4], the IoT primarily operates on three layers which are the Perception, Network, and the Application layer. Each layer of IoT has inherent security issues associated with it. Fig. 1 shows the basic three layer architectural framework of IoT with respect to the devices and technologies that encompass each layer.

2.1. Perception Layer

The perception layer is also known as the "Sensors" layer in IoT. The purpose of this layer is to acquire data from the environment with the help of sensors. This layer detects, collects, and processes information from sensors and then transmits it to the network layer. In addition, this layer may also performs IoT node collaboration in local and short range networks [3].

2.2. Network Layer

The network layer of IoT serves the function of data routing and transmission to different IoT hubs and devices over the Internet. At this layer, Internet gateways, switching, and routing devices etc. operate by using some of the very recent technologies such as WiFi, LTE, Bluetooth, 3G, Zigbee etc. to provide heterogeneous network services. The network gateways serve as the mediator between different IoT nodes by aggregating, filtering, and transmitting data to and from different sensors [4].

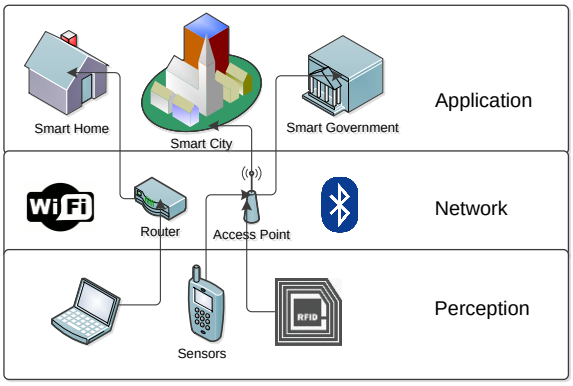

Figure 1. Three-layer IoT architecture

2.3. Application Layer

The application layer guarantees the authenticity, integrity, and confidentiality of the data. At this layer, the purpose of IoT which is the creation of smart environments is achieved.

3. IoT Security Issues

The same basic security goals of Confidentiality, Integrity and Availability that should be present for all communications using computers and networks are required to ensure the security of IoT. However, the IoT has many constraints and limitations in terms of the components and devices, computational and power resources, and even the heterogonous and ubiquitous nature of IoT that introduce additional concerns to be addressed with respect to establishing security. This section consists of two parts: the general security features that the IoT must have, and the security issues specific to each layer of the IoT.

3.1. The General Security Features of IoT

The security challenges of IoT can be broadly divided into two classes; Technological challenges and Security challenges [5]. The technological challenges arise due to the heterogeneous and ubiquitous nature of IoT devices, while the security challenges are related to the principles and functionalities that should be enforced to achieve a secure network. Table 1 shows some representative examples of challenges in both classes.

Security should be enforced in IoT throughout the development and operational lifecycle of all IoT devices and hubs [4]. There are different mechanisms to ensure security, some of which are given below:

- The software running on all IoT devices should be authorized.
- When an IoT device is turned on, it should first authenticate itself into the network before collecting or sending data.
- Since the IoT devices have limited computation and memory capabilities, firewalling is necessary in IoT network to filter packets directed to the devices.
- The updates and patches on the device should be installed in a way that additional bandwidth is not consumed.

Table 1. General IoT Security Challenges

Class	Challenges
Technological	Challenges related to wireless technologies, scalability, energy, and distributed nature of IoT
Security	Challenges to ensure security by authentication, confidentiality, end-to-end security, integrity etc.

Given below are the security principles that should be enforced to achieve a secure communication framework for the people, software, processes, and things in an IoT.

3.1.1. Confidentiality. It is important to ensure that data is secure and only available to authorized users. In IoT the term user includes human as well as machines and services, and it also includes the internal objects (devices that are part of the network) and external objects (devices that are not part of the network). For example, it is crucial to make sure that sensors do not reveal the collected data to neighboring nodes [6]. One more issue that must be addressed in the IoT security is how the data will be managed. It is important for the users of IoT to be aware of the data management mechanisms that will be applied, the process or person responsible for the management, and to ensure that the data is protected throughout the process [7].

3.1.2. Integrity. The IoT is based on exchanging data and information between many different types of devices, which is why it is important to ensure accuracy of the data; that data is being received from the right sender as well as to ensure that the data is not tampered with during the process of transmission due to intended or unintended interference. The integrity feature can be imposed by maintaining end-to-end security in IoT communications. The data traffic is typically managed by the use of firewalls and protocols, but these mechanisms do not necessarily guarantee the integrity at endpoints in IoT because of the low computational power at IoT nodes that do not support these mechanisms well.

3.1.3. Availability. The vision of IoT is to connect as many smart devices as possible. The users of the IoT should have all the data available whenever they need it. However data is not the only component that is used in the IoT; devices and services must also be reachable and available when needed in a timely fashion in order to achieve the expectations of IoT.

3.1.4. Authentication. Each object in the IoT must be able to clearly identify and authenticate other objects. However, this process can be challenging because of the nature of the IoT; many entities are involved (devices, people, services, service providers and processing units). In addition, sometimes objects may need to interact with other objects for the first time (objects they do not know) [8]. Because of all this, a mechanism to mutually authenticate entities in every interaction in the IoT is required.

3.1.5. Lightweight Solutions. All of the security goals mentioned earlier are not unique to IoT, although it may add special features and restrictions to each of them. However, in general confidentiality, integrity, availability and authentication are considered as basic goals in every computer or network security. Lightweight solutions on the other hand is a unique security feature that is introduced because of the limitations in the computational and power capabilities of the devices involved in the IoT. It is not a goal in itself but rather a restriction that must be considered while designing and implementing protocols either in encryption or authentication of data and devices in IoT. Since these algorithms or mechanisms are meant to be run on IoT devices with limited capabilities, so they ought to be compatible with device capabilities.

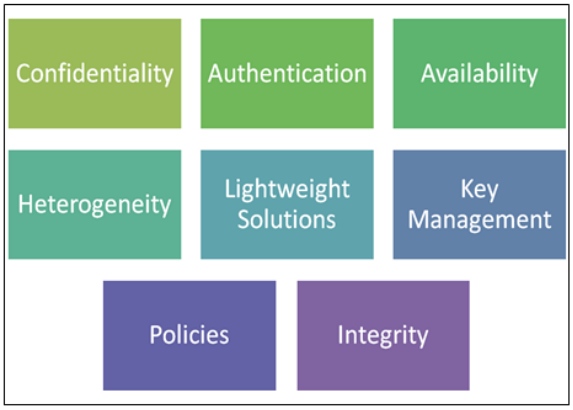

Figure 2. IoT security principles

3.1.6. Heterogeneity. The IoT connects different entities with different capabilities, complexity, and vendors. The devices even have different dates and release versions, use different technical interfaces and bitrates, and are designed for an altogether different functions. Therefore protocols must be designed to work in a variety of devices as well as in different situations [2, 4, 8]. The IoT aims at connecting device to device, human to device, and human to human, thus it provides connection between heterogeneous things and networks [5]. One more challenge that must be considered in IoT is that the environment is always changing (dynamics), at one time a device might be connected to a completely different set of devices than in another time. And to ensure security optimal cryptography system is needed with an adequate key management and security protocols.

3.1.7. Policies. There must be policies and standards to ensure that data will be managed, protected, and transmitted in an efficient way, but more importantly a mechanism to enforce such polices is needed to ensure that every entity is applying the standards. Service Level Agreements (SLO) must be clearly identified in every service involved. Current policies that are used in computer and networks security may not be applicable for IoT, due to its heterogeneous

and dynamic nature. The enforcement of such policies will introduce trust by human users in the IoT paradigm which will eventually result in its growth and scalability.

3.1.8. Key Management Systems. In IoT, the devices and IoT sensors need to exchange some encryption materials to ensure confidentiality of the data. For this purpose, there needs to be a lightweight key management system for all frameworks that can enable trust between different things, and can distribute keys by consuming devices' minimum capabilities.

3.2. Security Challenges in Each layer

Each IoT layer is susceptible to security threats and attacks. These can be active, or passive, and can originate from external sources or internal network owing to an attack by the Insider [1]. The active attack directly stops the service while the passive kind monitors IoT network information without hindering its service. At each layer, IoT devices and services are susceptible to Denial of Service attacks (DoS), which make the device, resource or network unavailable to authorized users. The security issues at each layer are stated in Table 2, and given below is a detailed analysis of these issues with respect to each layer.

3.2.1. Perception Layer. There are three security issues in IoT perception layer. First is the strength of wireless signals. Mostly the signals are transmitted between sensor nodes of IoT using wireless technologies whose efficiency can be compromised by disturbing waves. Secondly, the sensor node in IoT devices can be intercepted not only by the owner but also by the attackers because the IoT nodes usually operate in external and outdoor environments, leading to physical attacks on IoT sensors and devices in which an attacker can tamper the hardware components of the device. Third is the inherent nature of network topology which is dynamic as the IoT nodes are often moved around different places. The IoT perception layer mostly consists of sensors and RFIDs, due to which their storage capacity, power consumption, and computation capability are very limited making them susceptible to many kinds of threats and attacks [1, 9].

The confidentiality of this layer can easily be exploited by Replay Attack which can be made by spoofing, altering or replaying the identity information of one of the devices in IoT. Or the attacker might gain the encryption key by analyzing the required time to perform the encryption what is known as Timing Attack. Another confidentiality threatening attack is when the attacker takes over the node and captures all information and data which is basically Node Capture attack. Attacker can add another node to the network that threatens the integrity of the data in this layer by sending Malicious Data. This can also lead to a DoS attack, by consuming the energy of the nodes in the system and depriving it from the sleep mode that the nodes use to save the energy [6].

The above listed security issues at perception layer can be coped with by using encryption (which can be point-to-point or end-to-end), authentication (to verify true identity of sender) and access control [9]. Further security measures and protocols to address this issue are given in Section 4.

Table 2. Security Concerns at Each IoT Layer

Layer	Security Concerns and Threats
Perception	Wireless signal strengths, physical attacks, dynamic IoT topology
Network	Traffic analysis, eavesdropping, passive monitoring, heterogeneity of network components and protocols
Application	Absence of global and standard trust policies, authentication mechanisms

3.2.2. Network Layer. As mentioned before, the network layer of IoT is also susceptible to DoS attacks. Apart from the DoS attacks, the adversary can also attack the confidentiality and privacy at network layer by traffic analysis, eavesdropping, and passive monitoring [1]. These attacks have a high likelihood of occurrence because of the remote access mechanisms and data exchange of devices. The network layer is highly susceptible to Man-in-the-Middle attack, which can be followed by eavesdropping. If the keying material of the devices is eavesdropped, the secure communication channel will be completely compromised. The key exchange mechanism in IoT must be secure enough to prevent any intruder from eavesdropping, and then committing identity theft.

The communication in the IoT is different than that of the Internet because it is not restricted to machine to human. However, the feature of machine-to-machine communication that the IoT introduces has a security issue of Compatibility. The heterogeneity of the network components makes it difficult to use the current network protocols as is, and still produce efficient protection mechanisms. Attackers can also take advantage of the fact that everything is connected in order to gain more information about the users and use this information for future criminal activities [2]. Protecting the network is important in the IoT, but also protecting the objects in the network is equally important. Objects must have the ability to know the state of the network and the ability to protect themselves from

any attacks against the network. This can be achieved by developing protocols as well as software that enable objects to respond to any situations and behaviors that can be considered abnormal or may affect their security [7].

3.2.3. Application Layer. Since the IoT still does not have global policies and standards that govern the interaction and the development of applications, there are many issues related to the security. Different softwares and applications have different authentication mechanisms, which makes integration of all of them very difficult to ensure data privacy and identity authentication. The large amounts of connected devices that share data will cause large overhead on applications that analyze the data, which can have big impact on the availability of the services.

One more issue that must be considered when designing the applications in IoT is how different users will interact with them, the amount of data that will be revealed and who will be responsible for managing these applications. The users must have some tools to control what data they want to disclose and they must be aware of how the data will be used, by whom and when.

4. IoT Security Countermeasures

IoT requires security measures at all three layers; at physical layer for data gathering, at network layer for routing and transmission, and at application layer to maintain confidentiality, authentication, and integrity [4]. In this section the state-of-art security measures that address the specific features and security goals of IoT are discussed.

4.1. Authentication Measures

In 2011, Zhao et al. in [10] presented a mutual authentication scheme for IoT between platforms and terminal nodes. The scheme is based on hashing and feature extraction. The feature extraction was combined with the hash function to avoid any collision attacks. This scheme actually provides a good solution for authentication in IoT. The feature extraction process has the properties of irreversibility which is needed to ensure security and it is light weight which is desirable in IoT. The scheme focuses on authentication process when the platform is trying to send data to terminal nodes and not the opposite. Although the scheme will improve the security while keeping the amount of information sent reduced, it works only on theory and there is no practical proof of concept to support it.

Another method for ID authentication at sensor nodes of IoT is presented by Wen et al. in [9]. It is a one-time one cipher method based on request-reply mechanism. This dynamic variable cipher is implemented by using a pre-shared matrix between the communicating parties. The parties can generate a random coordinate which will serve as the key coordinate. Key coordinate is the thing which actually gets transferred between two parties, not the key itself. The key otherwise known as the password is then generated from this coordinate. All the messages are sent by encrypting them with the key, along with key coordinate, device ID, and timestamp. So, two devices communicate by validating timestamps, and thus they can cancel the session based on it. This cipher can be used where securing IoT is not very sensitive and crucial because key can be repeated for different coordinates. If key coordinate is changed regularly, security can be optimized for that particular IoT framework. The installation of pre-shared matrix needs to be secure for this work to be implemented for a large number of IoT devices.

Creating correct access controls is as important as authentication for security, and these two functionalities go hand in hand in securing IoT. To address these functionalities, Mahalle et al. [5] presented an Identity Authentication and Capability based Access Control (IACAC) for the IoT.

This research attempts to fill the gap for an integrated protocol with both authentication and access control capabilities to achieve mutual identity establishment in IoT. The proposed model uses a public key approach and is compatible with the lightweight, mobile, distributed, and computationally limited nature of IoT devices plus existing access technologies like Bluetooth, 4G, WiMax, and Wi-Fi. It prevents man-in-the-middle attacks by using a timestamp in the authentication message between the devices, which serves as the Message Authentication Code (MAC). The scheme works in three stages; first a secret key is generated based on Elliptical Curve Cryptography-Diffie Hellman algorithm (ECCDH) [11], then identity establishment is made by one-way and mutual authentication protocols, and lastly access control is implemented. The shared secret key is formed by the combination of public key and a private parameter, and has small size and low computational overhead due to the use of Elliptic curve cryptography (ECC). The access is granted by storing a capability with access rights, device identifier, and a random number in each IoT device. This random number is the result of hashing device ID with access rights. The IACAC model does not completely prevent DoS attacks. However, it minimizes it since access of resource is granted to only one ID at a time.

As discussed before, most of the devices involved in the perception layer of the IoT are RFID and sensors. Such devices have very limited computational capability, which makes it difficult to apply any cryptography algorithms to ensure the

security of the network. However, researchers in [12] introduced a light weight authentication protocol to secure RFID tags. In unsecured RFID the attacker can gain access to the network by sniffing the EPC (Electronic Product Key) of the victim tag and program it to another tag. By applying the authentication protocol such attacks can be prevented. The protocol ensures mutual authentication between RFID readers and tagged items without introducing large overhead on these devices.

4.2. Trust Establishment

Since, the things or devices in IoT can physically move from under one owner to a different one, trust should be established between both owners to enable a smooth transition of the IoT device with respect to access control and permissions. The work in [13] presents the concept of mutual trust for inter-system security in IoT by creating an item-level access-control framework. It establishes trust from the creation to operation and transmission phase of IoT. This trust is established by two mechanisms; the creation key and the token. Any new thing which is created is assigned a creation key by an entitlement system. This key is to be applied for by the manufacturer of the thing. The token are created by the manufacturer, or current owner, and this token is combined with the RFID identification of the device. This mechanism ensures the change of permissions by the device itself if it is assigned a new owner, or it is going to be operated in a different department of the same company, thus reducing the overhead of the new owner. These tokens can be changed by the owners, provided that old token is provided, so as to supersede the permissions and access control of the previous one. This mechanism is similar to changing the old key when a new home is bought.

4.3. Federated Architecture

Not having universal policies and standards to control the design and the implementation of algorithms in IoT makes it difficult to control the security. It is important for IoT to have a federated architecture that supports internal autonomy or a centralized unit to overcome the heterogeneity of various devices, softwares and protocols. The work in [14] suggested a definition for federated IoT, and based on that definition an access control delegation model is presented. The presented model takes into consideration the flexibility and scalability that are key features in IoT systems. Another such attempt was made in [15] to propose a framework called Secure Mediation GateWay (SMGW) for critical infrastructures. This approach is an abstraction of IoT as it is relevant for any kind of distributed infrastructures that are completely different in their nature and operation. SMGW can discover all the relevant distributed information from different nodes, and can overcome the heterogeneity of heterogeneous nodes whether it is a telecommunication, electrical, water distribution node, and can exchange all the messages and information over the untrusted network of Internet. This work enabled the follow-up of another federated approach, presented in [4] to provide the framework of Smart Home based on the SMGW.

It is not enough to have policies and standards to ensure security, mechanisms to enforce such policies are also needed. The research by Neisse et al. in [16] addresses this issue by integrating a security toolkit named SecKit with the MQ Telemetry Transport (MQTT) protocol. The current policies may not be efficient in IoT because of its dynamic nature. The proposed policy mechanism can have good impact in ensuring the security of the IoT, however it introduced additional delay in the process.

4.4. Security Awareness

Another important security measure for the success and growth of IoT framework is the awareness and concern among human users which are a part of IoT network. In [17] the authors explained the consequences of not securing the IoT using actual numbers. They accessed IoT devices (SCADA devices, web cameras, traffic control devices, and printers) that were publicly available using either no-password or the default password. The recorded results were very interesting and showed that many of these devices were actually accessible. If people continued with the same unawareness towards security, and used the minimum amount of security like default password that comes with the product, this would make the IoT to cause more harm than good. Hackers will gain more opportunities to conduct attacks against the whole network if one of its devices is not secured.

5. The Big Picture

IoT security is determined by the many factors and security principles discussed earlier, and the challenges that are faced by IoT security has been the focus of many researchers for long time. In this section, an analysis of some related work is presented and the contribution of this paper is given.
In survey paper presented by Roman et al. in [7], a detailed introduction about the IoT and security issues alongwith the need to have IoT standards are addressed. However, no countermeasures are provided for the given security challenges. This work was followed by the survey analysis in [8] in which countermeasures are provided for all security challenges. However, global policies for securing IoT and computational resources of security

solutions w.r.t. devices are not provided. The work in [2] attempts at describing the security issues at each layer with certain security measures. But, no solution is given except for encryption in perception layer. The analysis in [1] addresses the security threats, challenges, and requirements in detail, but presents state-of-art countermeasures for only one security feature of access control. In [6], IoT security in terms of the main principles of security like confidentiality, integrity, and availability are addressed only. The authors suggested two-step authorization using biometric which is not applicable in case of machine-to-machine communication. The suggested measures are not detailed and don't address the specific nature of IoT with low power heterogeneous devices and huge network traffic. A good survey for IoT, Web of Things (WoT), Social Web of Things (SWoT) is presented in [18], in which security issues, measures and potential research directions are given. In this survey paper, the security challenges, requirements, and state-of-art measures and research are presented with emphasis on using the latest network protocols like IPv6 and 5G to further secure the IoT paradigm.
The survey of state of art technologies to secure IoT shows that while a host of works provide countermeasures to cope up with different security challenges, but the scope of most of them is limited to authentication, identity establishment and access control functionalities.

Wireless Internet Service Provider roaming (WISPr) and RADIUS are the existing solutions to provide authentication and authorization in IoT by means of Wi-Fi over the Internet. Today, many smart devices support IPv6 communications, but the existing deployments in IoT might not support it, and thus requires ad-hoc gateways and middlewares [19]. This survey shows that open research challenges are present to achieve centralized autonomy in IoT devices by having a Management Hub that manages the identification management issues in IoT.

6. Future Directions

IoT has seen rapid development in recent years in the areas of telemedicine platforms, intelligent transportation systems, logistics monitoring, and pollution monitoring systems etc. Some analysts even believe that the number of things connected will increase up to 26 billion units by 2020 [4]. However, the security challenges related to the IoT must be dealt with to achieve its growth and maturation. Given below are future directions for research in order to make the IoT more secure.

6.1. Architecture Standards

IoT currently employs different devices, services, and protocols to achieve a common goal. However, to integrate a network of IoT frameworks to achieve a bigger framework, for example, to form a smart town by the integration of many smart homes, there needs to be a set of standards that should be followed from the micro to macro levels of IoT realization. The present day requirement of IoT is to have well-defined architecture standards comprising of data models, interfaces, and protocols that can support a wide range of humans, devices, languages, and operating systems.

6.2. Identity Management

The identity management in IoT is performed by exchanging identifying information between the things for first time connection. This process is susceptible to eavesdropping which can lead to man-in-the-middle attack, and thus can jeopardize the whole IoT framework. Hence, there needs to be some pre-defined identity management entity or hub which can monitor the connection process of devices by applying cryptography and other techniques to prevent identity theft.

6.3. Session layer

As per most of the researchers, the three-layer architecture of IoT does not accommodate the opening, closing, and managing a session between two things. So, there is a need for protocols which can address these issues and can ease the communication between devices. An abstract session layer should be accommodated as an additional layer in IoT architecture which can specifically manage the connections, protocols, and sessions between communicating heterogeneous devices.

6.4. 5G Protocol

To realize the implementation of IoT, IPv4 will definitely fall short in accommodating the huge numbers of IP-identifiable objects. That is the reason why there is a move towards implementing IPv6, which is able to support 3.4x1038 devices. However, such large number of devices will create a huge amount of traffic, which can lead to further delays and thus more bandwidth will be required. The expectation of the new generation of communication (5G) is to provide speed between 10-800Gbps, comparing this number with the current technology (4G) with speed of 2-1000 Mbps, 5G should be able to handle the traffic produced by IoT devices. 5G technology is also expected to accommodate both IPv4 and IPv6 by using IPv4/IPv6 framework translation. The implementation of 5G is being defined by many current and developing technologies such as: Heterogeneous Networks (HetNets), Software Defined Networks (SDNs), Massive MIMO, and Multiple Radio Access etc [20]. However, all of these technologies come with their

own security challenges. For example, HetNets will have frequent handover which directly affects the authentication process in the network, especially with the small latency requirement of 5G. Also, cloud computing and SDNs will increase the numbers of DDoS attacks due to the On-Demand Self-Service characteristic of cloud computing. Although [21] addressed the authentication and security of SDN by having a decentralized control of authentication using user-dependent security context, the security of 5G and all the emerging technologies involved in 5G must be extensively addressed, in order to ensure IoT security.

7. Conclusion

The IoT framework is susceptible to attacks at each layer. Therefore, there are many security challenges and requirements that need to be addressed. Current state of research in IoT is mainly focused on authentication and access control protocols, but with the rapid advancement of technology it is essential to incorporate new networking protocols like IPv6 and 5G to achieve the dynamic mashup of IoT topology.

The major developments witnessed in IoT are mainly on small scale including within companies and in some limited industries. To scale the IoT framework from one company to a cohort of different companies and different systems, various security concerns need to be addressed. The IoT has great potential to transform the way we live today. But, the foremost concern in realization of completely smart frameworks is security. If security concerns like privacy, confidentiality, authentication, access control, end-to-end security, trust management, global policies and standards are addressed completely, then a transformation of everything by IoT can be envisioned in the near future. There is need for new identification, wireless, software, and hardware technologies to resolve the currently open research challenges in IoT like the standards for heterogeneous devices, implementation of key management and identity establishment systems, and trust management hubs.

8. References

[1]M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[2]K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[3]L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[4]M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[5]P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[6]M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

[7]R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.

[8]R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

[9]Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 1062-1066, 2012.

[10]G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in Int'l Conference on Modelling, Identification and Control (ICMIC), 563-566, 2011.

[11]N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, 203-209, 1987.

[12]J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1-2, 2014.

[13]Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.

[14]B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604-608, 2012.

[15]M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5, 86-97, 2012.

[16]R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172, 2014.

[17]M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited Connections: A Study of

Vulnerable Devices on the Internet of Things (IoT)," in Joint Intelligence and Security Informatics Conference (JISIC), 232-235, 2014.

[18]I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for Interaction with Things on Internet and Underlying Issues," Ad Hoc Networks, 2015.

[19]S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, 146-164, 2015.

[20]W. H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," Wireless Communications, vol. 21, 106-112, 2014.

[21]X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," Communications Magazine, vol. 53, 28-35, 2015.

