# Introduction to IoT Security

Anca D. Jurcut, Pasika Ranaweera, Lina Xu
School of Computer Science
University College Dublin, Ireland
anca.jurcut@ucd.ie, pasika.ranaweera@ucdconnect.ie

***Abstract*** **-** In a world with "things" and devices interconnected at every level, from wearables to home and building automation, to smart cities and infrastructure, to smart industries, and to smart-everything, the Internet of Things (IoT) security plays a centric role with no margin for error or shortage on supply. Securing including authentication of these devices will become everyone's priority, from manufacturers to silicon vendors (or IP developers), to software and application developers, and to the final consumer, the beneficiary of the security "recipe" that will accompany these IoT products. Together, they need to adapt to the market demands, innovate and improve processes, grasp new skills and learn new methods, raise the awareness and elaborate new training and curricula programs.

In this chapter, we provide a thorough survey and classification of the existing vulnerabilities, exploitable attacks, possible countermeasures and the access control mechanisms including authentication and authorization. These challenges are addressed in detail considering both the technologies and the architecture used. Further, this work focuses also on IoT intrinsic vulnerabilities as well as the security challenges at every layer. Additionally, solutions for remediation of the compromised security, as well as methods for risk mitigation, with prevention and improvement suggestions are discussed.

***Index Terms*** – Internet of Things, Security, Attacks, Countermeasures, Authentication, Authorization

## 1 INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) into diverse application areas such as building and home automation, smart transportation systems, wearable technologies for healthcare, industrial process control and infrastructure monitoring and control is changing the fundamental way in which the physical world is perceived and managed. It is estimated that there will be about 30 billion IoT devices by 2020. Most of these IoT devices are expected to be of low-cost and wireless communication technology based, with limited capabilities in terms of computation and storage. As IoT systems are increasingly being entrusted with sensing and managing highly complex eco-systems, questions about the security and reliability of the data being transmitted to and from the IoT devices are quickly becoming a major concern.

It has been reported in several studies that IoT networks are facing several security challenges [1-7] including authentication, authorization, information leakage, privacy, verification, tampering, jamming, eavesdropping etc. IoT provides a network infrastructure with interoperable communication protocols and software tools to enable the connectivity to the internet for handheld smart devices (smart phones, personal digital assistants (PDA) and tabs), smart household apparatus (smart TV, AC, intelligent lighting systems, smart fridge, etc.), automobiles and sensory acquisition systems [1]. However, the improved

connectivity and accessibility of devices presents major concerns for security of all the parties connected to the network regardless of whether they are humans or machines. The infiltration launched by the Mirai malware on the Domain Name System (DNS) provider Dyn in 2016 through a botnet based DDoS attack to compromise IoT devices such as printers, IP cameras, residential gateways and baby monitors represents the fertility for cyber threats in the IoT domain [84]. Moreover, the cyber-attack launched at Ukrainian power grid in 2015 that targeted the Supervisory Control and Data Acquisition (SCADA) and caused a blackout for several hours is a prime exemplification on the gravity of devastation that could be resulted by modern day attacks [2]. The main reasons for the security challenges of current information centric automated systems is their insecure unlimited connectivity with the internet and the non-existent access control mechanisms for providing secure and trustful communication. Further, the problem of vulnerabilities in IoT systems arises due to the physical limitations of resource constrained IoT devices (in terms of computing power, on-board storage and battery-life), lack of consensus/standardization in security protocols for IoT, and widespread use of 3rd party hardware, firmware and software. These systems are often not sufficiently secure, especially when deployed in environments that cannot be secured/isolated through other means. The resource constraints on typical IoT devices make it impractical to use very complex and time-consuming encryption/decryption algorithms for secure message communication. This makes IoT systems highly susceptible to various types of attacks [1], [3], [4], [5], [6], [7]. Furthermore, addressing the security vulnerabilities in the protocols designed for communication is critical to the success of IoT [8], [9], [10], [11], [12].

This chapter focuses on security threats, attacks and authentication in the context of the IoT and the state-of-the-art IoT security. It presents the results of an exhaustive survey of security attacks and access control mechanisms including authentication and authorization issues existing in IoT systems, its enabling technologies and protocols, addressing all levels of the IoT architecture. We survey a wide range of existing works in the area of IoT security that use different techniques. We classify the IoT security attacks and the proposed countermeasures based on the current security threats, considering all three layers: perception, network and application. This study aims to serve as a useful manual of existing security threats and vulnerabilities of the IoT heterogeneous environment and proposes possible solutions for improving the IoT security architecture. State-of-the-art IoT security threats and vulnerabilities in terms of application deployments such as smart utilities, consumer wearables, intelligent transportation, smart agriculture, industrial IoT and smart city have been studied. The IoT security, particularly the IoT architecture, such as authentication and authorization, has also been investigated, considering all layers.

The remainder of this chapter is organized as follows. Section 2 provides the IoT classification of attacks and their countermeasures according to the IoT applications and different layers of the IoT infrastructure. Section 3 addresses the importance of authentication with respect to security in IoT and presents in details the existing authentication and authorization issues at all layers. Section 4 introduces other security features and the related issues. Additionally, solutions for remediation of the compromised security, as well as methods for risk mitigation, with prevention and improvement suggestions are discussed in the same section. A discussion on the content of the chapter regarding authentication mechanisms in the IoT domain with the state of the art methodologies has been presented in Section 5. Section 6 explicates future research directives such as blockchain, 5G, fog and edge computing, quantum, AI and network slicing. Finally, Section 7 concludes the study.

## 2 ATTACKS AND COUNTRAMEASURES

Security is defined as a process to protect a resource against physical damage, unauthorized access, or theft, by maintaining a high confidentiality and integrity of the asset's information and making information about that object available whenever needed. The IoT security is the area of endeavour concerned with safeguarding connected devices and networks in the Internet of Things environment. IoT enables to improve several applications in various fields, such as, smart cities, smart homes, healthcare, smarts grids, as well as other industrial applications. However, introducing constrained IoT devices and IoT technologies in such sensitive applications leads to new security challenges.

IoT is relying on connectivity of myriads of devices for its operation. Hence, the possibility of being exposed to a security attack is most probable. In IT, an attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to an asset. For example, cryptographic security protocols are a key component in providing security services for communication over networks [10]. These services include data confidentiality, message integrity, authentication, availability, nonrepudiation, privacy [3]. The proof of a protocol flaw is commonly known as an "attack" on a protocol and it is generally regarded as a sequence of actions performed by a dishonest principal, by means of any hardware or software tool, in order to subvert the protocol security goals. An IoT attack is not peculiar from an assault against an IT asset. What is new is the scale and relative simplicity of attacks in the Internet of Things (IoT) - the millions and billions of devices that are a potential victim of traditional style cyber-attacks, but on a much larger scale and often with limited or no protection.

The most prevalent devices which are connected to serving IoT applications for infotainment purposes are smart TVs, webcams and printers. A vulnerability analysis has been conducted in [83] on these devices using Nessus[1] tool to observe that approximately 13% of the devices out of 156,680 were attributing vulnerabilities which were further classified as critical, high, medium and low. The vulnerabilities that exist in such as MiniUPnP, NAT-PMP detection, unencrypted telnet, Simple Network Management Protocol (SNMP) agents, Secure Shell (SSH) weak algorithms and File Transfer Protocol (FTP) inherited by webcams, smart TVs and printers are further identified based on manufacturer models.

In this section, we present the results of our study on the existing vulnerabilities, exploitable attacks and possible countermeasures in the context of the IoT and the state-of-the-art IoT security. We surveyed a wide range of existing work in the area of IoT security that uses different techniques. We classified the IoT security attacks and the proposed countermeasures based on the current security threats, considering all three layers: Perception, Network and Application. The Figure 1 illustrates the typical architecture of IoT and entities which are considered under each layer. Table 1 summarizes the taxonomy of attacks and viable solutions of IoT categorized under each layer. These attacks and their corresponding solutions will be further discussed below.

[1] https://www.tenable.com/products/nessus/nessus-professional

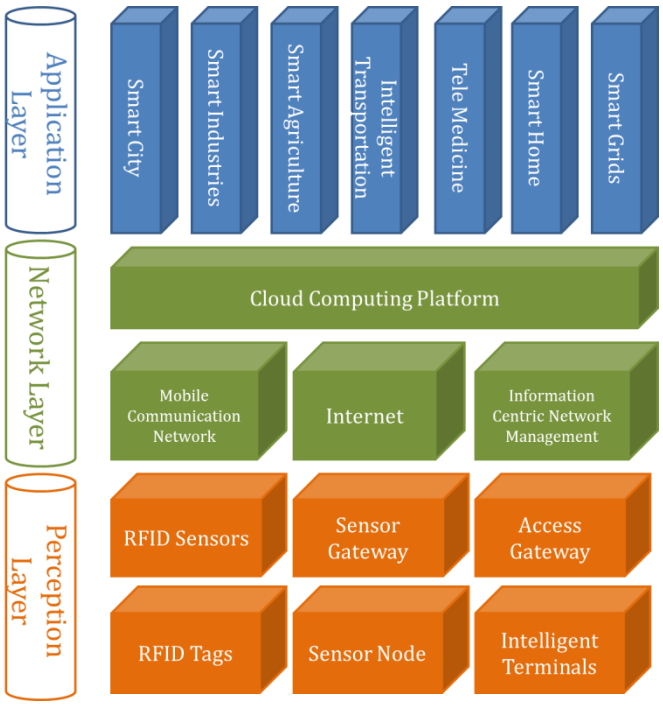


Figure 1 - IoT architecture

Table 1 - Taxonomy of attacks and solutions in IoT layers

| | **LAYER/ COMPONENT** | **ATTACKS** | **SOLUTIONS** |
|---|---|---|---|
| a. | **PERCEPTION LAYER** | | |
| | *Perception Nodes RFID* | Tracking, DoS, repudiation, spoofing, eavesdropping, data newness, accessibility, self-organization, time management, secure localization, tractability, robustness, privacy protection, survivability and counterfeiting [13]. | Access control, data encryption which includes non-linear key algorithms, IPSec protocol utilization, cryptography techniques to protect against side channel attack [9], [14], Hashed based access control [15], Ciphertext re-encryption to hide communication [16], New lightweight implementation using SHA-3 appointed function Keccak-f (200) and Keccak-f (400) [17] |
| | *Sensor nodes* | Node subversion, node failure, node authentication, node outage, passive information gathering, false node message corruption, exhaustion, unfairness, sybil, jamming, tampering and collisions [18][19] | Node authentication, Sensor Privacy |

| | | | |
|---|---|---|---|
| | *Sensor Gateways* | Misconfiguration, hacking, signal lost, DoS, war dialling, protocol tunnelling, man-in-the-middle attack, interruption, interception and modification fabrication [20] | Message Security, Device Onboard Security, Integrations Security [21] |
| b. | **NETWORK LAYER** | | |
| | *Mobile Communication* | Tracking, eavesdropping, DoS, bluesnarfing, bluejacking, bluebugging alteration, corruption and deletion [1], [5], [40] | Developing secure access control mechanisms to mitigate the threats by employing biometrics, public-key crypto primitives and time changing session keys. |
| | *Cloud Computing* | Identity management, heterogeneity which is inaccessible to an authentic node, data access controls, system complexity, physical security, encryption, infrastructure security and misconfiguration of software [22] | **Identity privacy** - Pseudonym [23, 24, 25], group signature [24], connection anonymization [26, 31]<br>**Location privacy** - Pseudonym [23, 24, 25], one-way trapdoor permutation [27, 28]<br>**Node compromise attack** - Secret sharing [28, 29, 30], game theory [26], population dynamic model [28]<br>**Layer removing/adding attack** - Packet transmitting witness [25, 28, 31], aggregated transmission evidence [28]<br>**Forward and backward security** - Cryptographic one-way hash chain [23, 24]<br>**Semi-trusted/malicious cloud security** - (Fully) homomorphic encryption [32], zero knowledge proof [33] |
| | *Internet* | Confidentiality, encryption, viruses, cyberbullying, hacking, identity theft, reliability, integrity and consent [34] | Identity Management for confidentiality [35], Encryption schemes for confidentiality of communication channels [36], Cloud based solutions to establish secure channels based on PKI for data and communication confidentiality [36] |
| c. | **APPLICATION LAYER** | Data privacy, Tampering Privacy, Access control, disclosure of information [18] | Authentication, key agreement and protection of user privacy across heterogeneous networks [37], Datagram Transport Layer Security (DTLS) for end-to-end security [38], Information Flow Control [29] |

## 2.1 PERCEPTION LAYER

The devices belonging to perception layer are typically deployed in Low-power and Lossy networks (LLN), where energy, memory and processing power are constricted compared to localization of network nodes in conventional internet platforms [1]. Therefore, including secure public key encryption based authentication schemes would be infeasible due to their requirement of high computational power and storage capacity. Hence, developing a lightweight cryptographic protocol would be a challenging task when scalability, context-awareness and ease of deployment should also be considered [2].

There are several problems and attacks to be considered for the perception layer. We will be addressing these as showed in Table 1 by discussion the existing problems and attacks for perception nodes, sensor nodes and sensor gateways.

### 2.1.1 Perception nodes

RFID nodes and tags are used as perception nodes typically. RFID tags could be subjected to Denial of Service (DoS - from radio frequency interference), repudiation, spoofing and eavesdropping attacks in the communication RF channel [1], [6], [13]. Moreover, reverse engineering, cloning, viruses (SQL injection attack in 2006), tracking, killing tag (using a pre-defined kill command to disable a tag), block tag (employing a jammer such as a Faradays' cage) and side channel attacks through power analysis are attacks which could compromise the RFID physical systems [86]. These attacks are feasible due to the low resources of RFID devices and comparatively weaker encryption/ encoding schemes. Solutions to overcome these vulnerabilities and the corresponding exploitable attacks include access control, data encryption which includes non-linear key algorithms, IPSec protocol utilization, cryptography techniques to protect against side channel attacks [9], [14], hashed based access control [15], ciphertext re-encryption to hide communication [16], new lightweight implementation using SHA-3 appointed function Keccak-f (200) and Keccak-f (400) [17].

### 2.1.2 Sensor nodes

Sensor nodes, such as ZigBee, possess additional resources compared to RFID devices with a controller for data processing and interoperability of sensor components, a Radio Frequency (RF) transceiver, a memory, the power source and the sensing element [1]. Even though the sensor nodes follow a fairly secure encryption scheme due to the elevated resources, attacks such as node tampering, node jamming, malicious node injection, Sybil and collisions [18], [19] could exploit the vulnerabilities in the nature of transmission technology and remote / distributed localization of them. A malware exploiting a flaw in the radio protocol of ZigBee caused a SOS code illumination in smart Philips light bulbs as a demonstration of weakness in sensor node systems in 2016 [84]. Additionally, GPS sensors are vulnerable to jamming or data level and signal level spoofing which results in Time Synchronization Attacks (TSA) targeted on Phasor Measurement Units (PMUs) of various IoT deployments that rely on GPS for locating or navigation based services [87]. Possible countermeasures for such attacks are node authentication and sensor privacy techniques.

### 2.1.3 Gateways

Sensory gateways are responsible for checking and recording various properties such as temperature, humidity, pressure, speed, and functions of distributed sensor nodes. User access, network expansion, mobility, and collaboration are provided using sensor gateways.

These channels are also vulnerable to several attacks such as misconfiguration, hacking, signal lost, DoS, war dialling, protocol tunnelling, man-in-the-middle attack, interruption, interception and modification fabrication [20]. Moreover, perception layer devices could be subjected to Side Channel Attacks (SCA) such as Differential Power Analysis (DPA), Simple Power Analysis (SPA), timing and acoustic cryptanalysis [6]. To ensure security with respect to sensory gateways, message security, device on board security and integrations security are suitable proposed solutions [21].

## 2.2 NETWORK LAYER

Network Layer facilitates the data connectivity to perception layer devices for accomplishing the functionality of various applications in the Application layer. Due to this layer being the connectivity provider for other layers, there are probable security flaws which would compromise the operations of the entire IoT architecture.

### 2.2.1 Mobile Communication

Mobile devices are the main interfaces of human interaction for IoT technology which ranges from smart phones, PDAs to mini-PCs. The state of the art for the mobile devices is extensively resourceful with their location services, biometric sensors, accelerometer / gyroscope, extended memory allocations, etc. The connectivity options are ranging from RF, Low Rate Wireless Personal Area Networks (LR-WPAN / IEEE 802.15.4), Near Field Communication (NFC), Wireless Fidelity (Wi-Fi) to Bluetooth. Though, these devices are vulnerable to DoS, sinkhole, bluesnarfing, bluejacking, blue bugging, alteration, corruption, deletion of data, and traffic analysis attacks [1], [5], [6], [40]. In addition, mobile devices are vulnerable for phenomena such as cloning, spoofing and various battery draining attacks explicated in [85]. Even the technologies LR-WPAN, Bluetooth and Wi-Fi are vulnerable to data transit attacks [84]. However, current standards of mobile devices have the means for improving the security through developing secure access control mechanisms to mitigate the threats by employing biometrics, public-key crypto primitives and time changing session keys.

### 2.2.2 Cloud Computing

Cloud computing platform is the prime entity in IoT for centralized processing and storage facilitation for IoT applications. Through cloud computing, IoT applications could enable higher computing power with unlimited storage capacity for a low cost, while maintaining a versatile accessibility. Reliance on standalone dedicated server based services is superseded by remote cloud based server farms with outsourced services. However, outsourcing information to be stored in a remote location could raise security concerns. Privacy preservation is the most inevitable issue with cloud computing among other flaws such as physical security, anonymity, data access control failure, identity management, and direct tampering of the cloud servers [1], [22]. Several security solutions have been proposed in different areas for cloud including: (1) Identity privacy - Pseudonym [23], [24], [25], group signature [24], connection anonymization [26], [31]; (2) Location privacy - Pseudonym [23], [24, [25], one-way trapdoor permutation [27], [28]; (3) Node compromise attack - Secret sharing [28], [29], [30], game theory [26], population dynamic model [28]; (4) Layer removing/adding attack - Packet transmitting witness [25], [28], [31], aggregated transmission evidence [28]; (5) Forward and backward security - Cryptographic one-way hash chain [23], [24]; (6) Semi-trusted/malicious cloud security - (Fully) homomorphic encryption [32], zero knowledge proof [33].

### 2.2.3 Internet

The term Internet stands for the holistic global networking infrastructure which scopes from private, public, academic, cooperate networks to government networks [1]. The connectivity through the Internet is formulated by Transmission Control Protocol / Internet Protocol (TCP/IP) and secured through various protocols such as Secure Socket Layer (SSL) / Transmission Layer Security (TLS), IPSec and Secure Shell (SSH). Though in IoT, Datagram Transport Layer Security (DTLS) is used as the communication protocol [1]. Since the Internet is accessible for everyone, the amount and nature of vulnerabilities out-weight the effectiveness of existing secure communication protocols [3], [4], [5], [7], [8], [10], [11] due to its implosive access capacity. Probable attacks are viruses, worms, hacking, cyber bullying, identity theft, consent and Distributed DoS (DDoS) [1], [34]. Countermeasures to overcome these attacks include Identity Management for confidentiality [35], Encryption schemes for confidentiality of communication channels [36], Cloud based solutions to establish secure channels based on PKI for data and communication confidentiality [36].

## 2.3 APPLICATION LAYER

As illustrated in Figure 2, possible applications for IoT are expanded into every industry available in the current era in addition to myriads of non-industrial applications developed for automation purposes. In general, feasible attacks in IoT application layer could be represented in two forms. They are software based and encryption based attacks. In the software attacks, most attacks are based on malicious software agents, apart from the phishing attacks in which the attacker reveals the authentication credentials of the user by impersonating as a trusted authority. Malware, worms, adware, spyware and Trojans are highly probable occurrences with the heterogeneity of IoT applications and their broader services [6]. Encryption based attacks are the approaches taken to exploit the procedural nature of the cryptographic protocols and their mathematical model through extensive analysis. Cryptanalytic attacks, ciphertext only attacks, known plaintext attacks and chosen plaintext attacks exemplify such possible threats [18].

There are several solutions proposed in the literature for the security of IoT applications such as Authentication, key agreement and protection of user privacy across heterogeneous networks [37], Datagram Transport Layer Security (DTLS) for end-to-end security [38], Information Flow Control [29]. The countermeasures for software based authentication should be taken for mitigating attacks such as phishing attacks, through verifying the identity of malicious adversaries before proceeding.

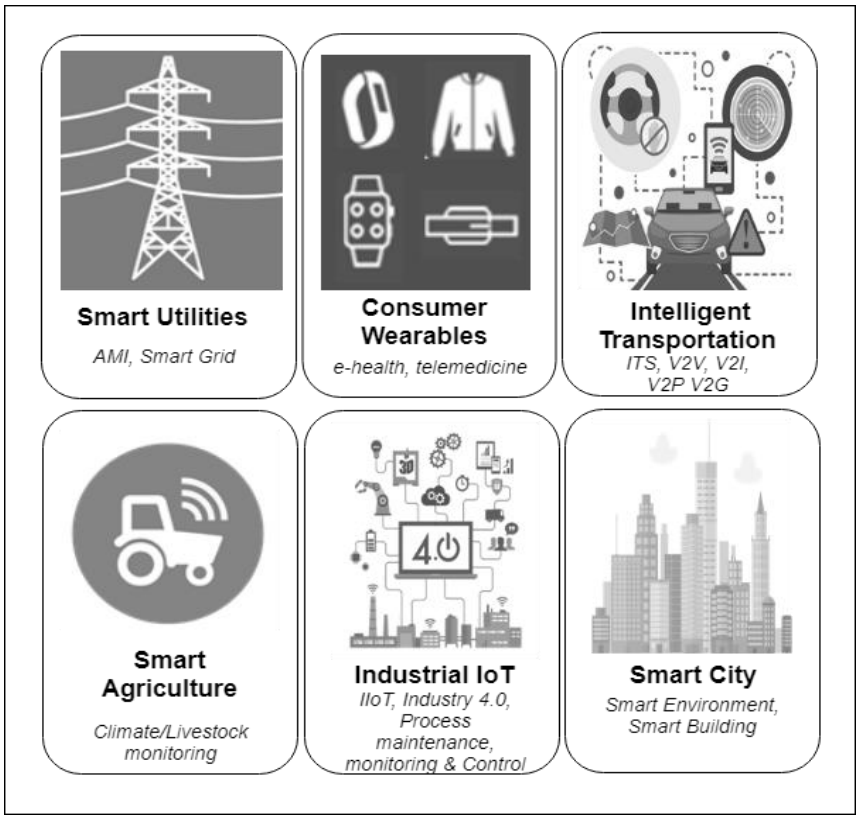


Figure 2 – IoT Applications

### 2.3.1 Smart Utilities – Smart Grids and Smart Metering

Smart Grids are the future of energy distribution for all the industrial and residential sectors. IoT plays a major role in smart grids for establishing the communication and monitoring protocols with the consumers of energy. Smart grid is a decentralized energy grid with the ability to coordinate the electricity production in relation to the consumption or consumption patterns of the consumer. It has a monitoring technology Advanced Metering Infrastructure (AMI) / smart metering / net metering, which can measure and update the power consumption parameters to both entities in real time [41]. Additionally, smart grids are incorporating renewable energy sources commissioned in consumer vicinity to cater the bidirectional energy flow for mitigating energy deficiencies [1].

Figure 3 illustrates a Smart Grid Architectural Model (SGAM) proposed by the coordinated group of European Committee for Standardization - European Committee for Electrotechnical Standardization - European Telecommunications Standards Institute (CEN-CENELEC-ETSI), which offers a framework for smart grid use cases [78]. This architecture formulates three dimensions which concatenate five functional interoperability layers with energy sector domains and zones which accounts for power system management [79]. This holistic framework is capable of reinforcing the designing stages of the smart energy systems. The IoT technologies could be amalgamated with the SGAM framework to establish the bi-directional communication.

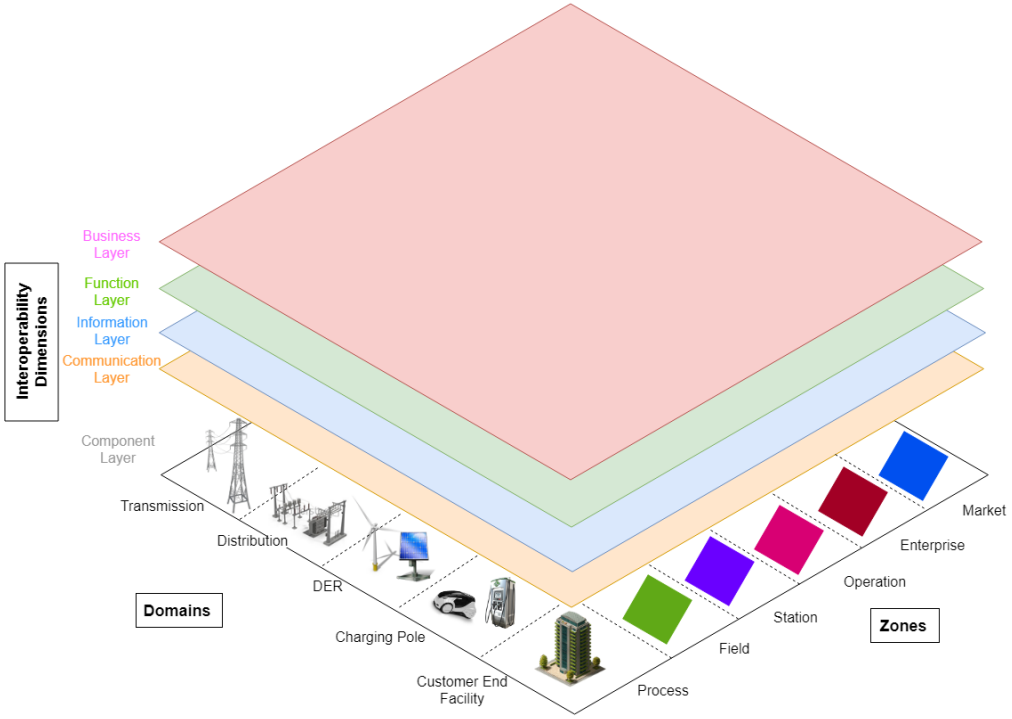


Figure 3 - Smart grid architectural model

All the monitoring applications are developed with IoT infrastructure with grid controlling access granted to the grid controlling officers for pursuing configurations while the consumers could only visualize the consumption details via a mobile device. The information circulated through the AMI would pose a privacy concern for consumers for disseminating information regarding their habitual activities, where the impact could be severe for industries. Due to the heterogeneous nature of communication equipment deployed with IoT and rapidly increasing population and industries, it would cause scalability issues for security. Smart girds are distributed across the power serving area and are exposed to adversaries.

As the energy distribution system is the most critical infrastructure that exists in an urban area, the conversion of the current power line communication (sending data over existing power cables) based controlling and monitoring channels to the wireless medium with the introduction of IoT technologies would expose the entire system into unintended security vulnerabilities. The intruders could perpetuate AMI interfaces stationed at every household or industrial plant with proper techniques. Once the access is granted to the hostile operators, potential outcomes could be devastating as to the level of disrupting the energy flow of a local grid substation to overloading a nuclear reactor of a power station. The availability of the grid could be compromised from IP spoofing, injection and DoS / DDoS attacks [41]. Thus, access controlling for devices used in AMI and grid controlling system should be secured with extra countermeasures.

### 2.3.2 Consumer wearable IoT (WIoT) devices for healthcare and telemedicine

IoT based healthcare systems are the most profitable and funded projects in the entire world. This is mainly due to the higher aggregate of aging people since health is the most concerned aspect of human life. A sensory system embedded with actuators is provided for individuals to use as a wearable device (i.e WIoT device) illustrated in Figure 4. WIoT device is used for tracking and recording vitals such as blood pressure, body temperature, heart rate, blood sugar, etc., [41]. This data would be conveyed and stored in a cloud as a Personal Health Record (PHR) in order to be accessed by the user and the assigned physicians.

Figure 4 – WIoT devices

IoT based healthcare systems are the most profitable and funded projects in the entire world. This is mainly due to the higher aggregate of aging people and health is the most concerned aspect of human life. A sensory system embedded with actuators are provided for individuals to use as a wearable device called as WIoT device which are illustrated in Figure 4 for tracking and recording vitals such as blood pressure, body temperature, heart rate, blood sugar along with exercises carried out by them [41]. This data would be conveyed and stored in a cloud as a Personal Health Record (PHR) to be accessed by the user and the assigned physicians.

Since the data handled in IoT based healthcare is personal, privacy is the most demanding security issue. Hence, the access control mechanism for wearable devices as well as for PHRs should be well secured. However, employing strong crypto primitives for enhancing the authentication protocols of PHRs is possible since they are stored in cloud environments. Hence, the same privacy concerns presented in section 3.2.2 under cloud computing apply. Moreover, a method for assuring anonymity of patients should be developed in case the PHRs are exposed to external parties, since they are stored in Cloud Service Providers (CSPs). Wearable devices face the resource scarcity issues for battery power, memory and processing level [41]. Thus, a lightweight access control protocol should be employed. Similar to all the other IoT applications, heterogeneous wearable devices produced by different manufacturers would employ diverse technologies for developing communication protocols. Thus, developing a generic access control policy would be extremely challenging.

### 2.3.3 Intelligent Transportation

Intelligent Transportation Systems (ITS) are introduced to improve transportation safety and degrade traffic congestions while minimizing the environmental pollution. In an ITS system, there are four main components such as vehicles, road side stations, ITS monitoring centre and security system [41]. All the information extracted from vehicular nodes and road side stations are conveyed to the ITS monitoring center for further processing, while the security subsystem is responsible for maintaining overall secureness. The entire system could be considered as a vehicular network, while the communications are established between Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P) and Vehicle-to-Grid (V2G) [41]. These communication links are implemented using technologies like RFID and Dedicated Short Range Communication (DSRC) for launching a large Wireless Sensor Network (WSN) [1]. The vehicular nodes and the entire data storing and monitoring infrastructure form a viable IoT deployment.

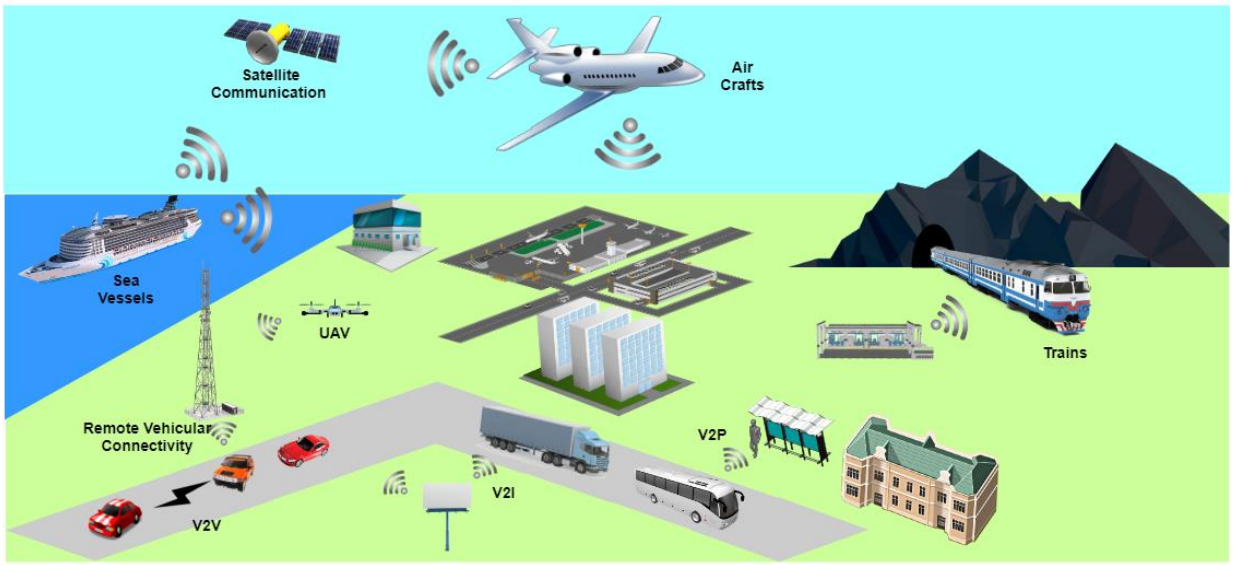


Figure 5 - Intelligent Transportation System

Figure 5 illustrates an ITS model, which enables communication among vehicular entities travelling through different mediums (airborne, land and marine) with various technologies such as satellite, mobile, Wireless Local Area Network (WLAN), etc. Such a system would enable services like real time updated navigation, roadside assistance, automated vehicular diagnostics, accident alerting system and self-driving cars [80]. Thus, massive divergence in the applicability of ITS deployment raises the requirement for a ubiquitous wireless connectivity with access points.

As mentioned above, a larger number of entry points to a vehicular network makes it vulnerable to diverse attacks to be targeted at many sources [41]. At the same time privacy of drivers should be ensured from external observers, though the drivers are not participating in any authentication activity. Authentication mechanisms are initiated between V2V interfaces where they could be exploited by an invader impersonating as another vehicle or a road side station. Therefore, a mechanism to verifying the identity of the vehicles or road side stations should be developed as a Trusted Third Party (TTP) with the authentication mechanism.

In some V2V communication systems, On Board Diagnostic (OBD) unit is utilized to extract information directly from Engine Control Unit (ECU) [1]. OBD port could be used to manipulate the engine controls of a vehicle and could be remotely accessed via the systems being developed. Thus, securing the access to the OBD port is vital.

### 2.3.4 Smart Agriculture

Agriculture is the most crucial industry in the world as it does produce food and beverages by planting crops such as corn, paddy, wheat, tea, potatoes, oats, etc. With the rapid population growth around the world and accounting the resource depletion, pollution and scarcity for human labor; agriculture is becoming an arduous industry. The automation is the most probable alternative for improving the effectiveness of the agriculture industry. Thus, IoT could play a vital role in automating. IoT infrastructure could be deployed to perform climate/ atmospheric, crop status monitoring and livestock tracking. Climatic sensors, water/ moisture level sensors and chemical concentration / acidity sensors along with visual sensors could be deployed for crop status monitoring, while automated water and fertilizer dispersing mechanisms are in place within the bounds of the plantation. Additionally, livestock tracking is another aspect of smart farming implemented through deploying Local Positioning Systems (LPSs) on farm animals.

This sort of a smart system would provide the benefits such as the ability to utilize the fertilizer and water usage while maximizing the crop production by mitigating the effects from climatic deficiencies. The fruition science and 'Hostabee' are two use cases of smart agriculture solutions used currently by the plantation industry [80].

Due to the diverse nature of sensor devices used in smart agriculture applications, integrating them into a holistic system could raise concerns considering the compatibility of technologies among varied manufacturers and protocols in which the communication is established. As the plantations or fields are extending to larger areas, number of IoT enabled sensory systems to be deployed should be immense. Handling the data flow of such a large number of individual sensors with different data representations dispersed through a broadened geographical region exerts the requirement for a communication technology with a higher coverage and moderate data rates which could not be satisfied by low range communication technologies such as Bluetooth or NFC. However, DSRC would be a suited technology to create a WSN with smart agriculture sensors, as it is compatible with ITSs.

As the IoT devices are disseminated to a larger geographical extent, probability of any IoT device being compromised is high as they are exposed. The perception level attacks are probable with these devices as they are sensory nodes and would be scarce of resources for both processing and storing information. The spoofing, impersonation, replay and Man-in-the-Middle (MiM) attacks are probable with this application [82]. This urges for a proper authentication scheme as all the perception level attacks could be mitigated with such a countermeasure.

### 2.3.5 Industrial IoT (IIoT)

M2M based automation systems are quite common for industries such as oil and gas manufacturers. These industries are vast and the machinery employed is massive, expensive and poses a significant risk to machine operators. The functions such as oil exploration by drilling, refining and distributing are all conducted using automated machinery controlled through Programmable Logic Controller (PLC) based on SCADA systems. Though, the current M2M infrastructure is ideal for controlling the machinery, remote monitoring and accessibility is limited while a proper data storage and processing mechanism for decision making is unavailable. Thus, the requirement for IoT arises to improve the operational efficiency by optimizing the robot controlling, reducing downtime through predictive and preventive maintenance, increasing productivity and safety through real time remote monitoring of assets [80]. IoT sensor nodes could be deployed at the machinery while monitoring tools could be integrated without affecting the operation of SCADA systems. Hence, SCADA system could be optimized to enhance the productivity.

The Smart Factories term is an adaptation of IIoT, introduced as "Industry 4.0" to represent the Fourth Industrial Revolution (4IR) [81]. This standard signifies a trend of automation and data exchange in manufacturing industries which integrates Cyber-Physical Systems (CPS), IoT and Cloud Computing based Data analytics [81],[80]. The interoperability, information transparency, technical assistance and decentralize decision making are the design principles of Industry 4.0 standard. BOSCH has developed connected hand held tools which could monitor location, current user, and task at hand type of accessories that are used such as the screw and that records the usage statistics for future references [80]. Thus, the deployment of IoT at industries is imminent in the future.

The security of the industrial applications is a major concern, as any hostile intrusion could result in a catastrophic occurrence for both machinery and human operators. The SCADA systems are no longer secure (E.g. considering the recent events [2]) due to their isolated localization and operation. However, main controlling functions are maneuvered within the control station located inside the industrial facility, while limited egress connectivity is maintained via satellite links with VSAT (Very Small Aperture Terminal) or microwave in case of offshore or any other industrialized plants of such nature.

Due to their offline nature, the probability of any online intrusion is minimal. Though, any malicious entity such as a worm or a virus injected to the internal SCADA network could compromise the entire factory. Once inserted into the system, the intention of the malicious entity would be to disrupt the operations of the facility and its machinery. Thus, limiting the possibility for any malicious insurgence from the internal network and employing effective Intrusion Detection System (IDS) to detect malicious entities, would be the most suited countermeasures for this application.

### 2.3.6 Smart Buildings, Environments and Cities

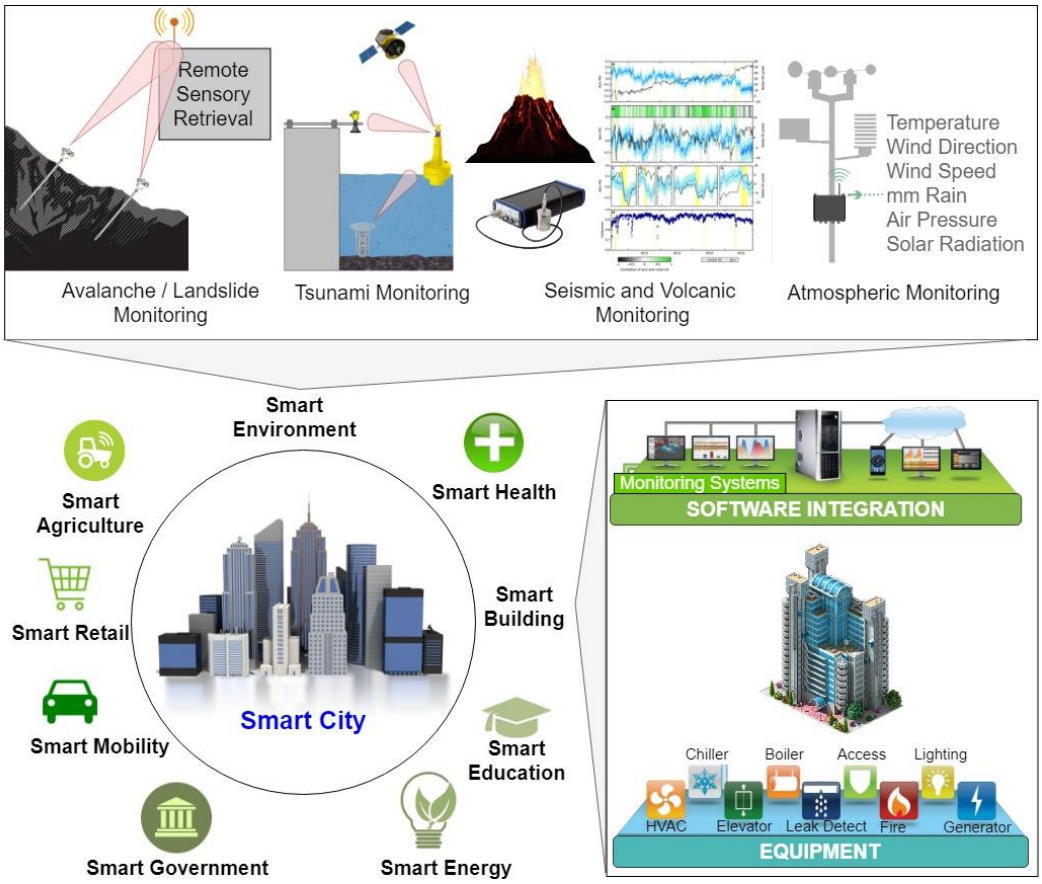


Figure 6 – Smart City Concept

Smart city is a holistically expanded inclusion of smart buildings and smart environments along with other smart automation systems formed for improving the quality of life for residents in a city. This is in fact the most expandable version of any IoT application in terms of cost for infrastructure deployment and geographical extent. In this concept, as shown in Figure 6, sensors are deployed throughout the building, environment or the city for the purpose of extracting data of parameters varied from temperature, humidity, atmospheric pressure, air density / air quality, noise level, seismic detection, flood detection and radiation level. CCTV streams and LPSs would be a valuable input for smart building and smart cities for detecting intrusions, monitoring traffic and emergencies. All other smart systems explained in the previous sections are in fact subsystems of a functional smart city.

Due to various parameters to be gathered from the sensory acquisitions, heterogeneity is immense and the implementation is arduous [41]. At the same time, management of the gathered Big Data content is not scalable. Thus, providing security for all the applications in smart cities would be extremely challenging. Most of the Big Data content extracted from the sensors is forwarded to clouds through M2M authentication. Due to large data transmissions, cryptographic schemes should be lightweight and the authentication mechanism should be dynamic. DoS or DDoS attacks are most probable and could be mitigated with a strong authentication mechanism [1]. Individual sensors could be compromised to initiate fake emergencies and access control methods should be improved to avoid such inconsistencies at sensor level.

The paper [42] introduces applications of IoT with specific focus on smart homes. The study presented in [42] claims that although smart homes are offering comfortable services, security of data and context-oriented privacy is also a major concern of these applications. The security and privacy issues in IoT applications have also been studied in [43].

# 3 AUTHENTICATION AND AUTHORIZATION

Authentication and access control mechanisms hold a great deal of significance in IoT. Without a proper mechanism for access control, entire IoT architecture could be compromised, since IoT devices are highly reliant on the trustfulness of the other components that are connected with. Thus, a proper access control mechanism is paramount to mitigate the flaws in the current IoT infrastructure.

Access control mechanisms are comprised of two stages (Figure 7) [1]: (1) Authentication and (2) Authorization.

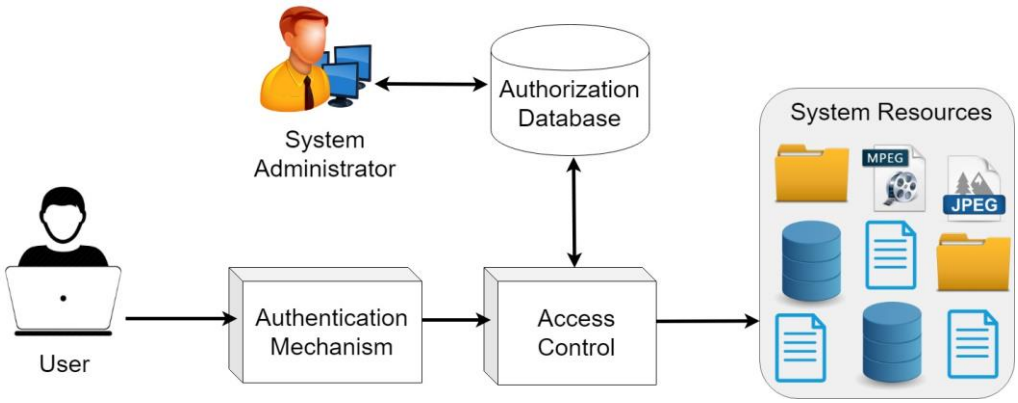


Figure 7 – Typical Access Control System

## 3.1 AUTHENTICATION

Authentication is the process of verifying the identity of an entity [2]. The entity to be verified could either be a human or a machine. Authentication is the first phase of any access control mechanism which can determine the exact identity of the accessing party in order to establish the trust of the system. In most cases, authentication is initiated between a human and a machine in process to log into the internet banking portal entering the credentials. However, in this scenario the access seeking entity does not have a guarantee regarding the identity of the access granting entity. In order to overcome this concern, mutual-authentication should be established between the entities, by verifying the identity of the access granting entity with the involvement of a TTP, such as a Certificate Authority (CA) [2]. CAs are globally recognized institutions which are responsible for issuing and maintaining secure digital certificates of web entities registered under them. These certificates are imperative for the operation of all modern day authentication protocols such as SSL/TLS, IPSec and HTTPS.

The process of authentication is merely facilitating credentials of an entity to the access granting system, which are unique to that entity and could only be possessed by them. This mechanism could be enabled with or without a TTP. The credentials used are often categorized as factors. The authentication schemes accuracy and efficiency depends on the number of factors that are engaged in the mechanism. The types of factors are listed below.

- Knowledge factor – passwords, keys, PINs, patterns
- Possession factor – Random Number Generators (RNG), ATM card, ID card
- Inherence factor – Biometrics such as fingerprint, palm print, iris, etc.

Recent innovations in embedding biometric sensors to smart handheld devices have enabled the possibility of using multi-factor multi-mode (if more than one bio metric is used for verification) Human-to-Machine (H2M) authentication protocols for IoT devices. Though, Machine-to-Machine (M2M) authentication could only be conducted using cryptographic primitives. However, including strong cryptographic primitives (Public Key Infrastructure (PKI), Hashing, Timestamps, etc.) for the authentication protocols involved is crucial in order to ensure data confidentiality, integrity and availability, as the credentials being conveyed are highly sensitive and unique for the authenticating entity.

### 3.2 AUTHORIZATION

Authorization is the process of enforcing limits and granting privileges to the authenticated entities [44]. In simple terms, this is determining the capabilities of an entity in the system. In order for an entity to be authorized for performing any action, the identity of that entity should be verified first through authentication. According to Figure 7, usually an administrator is configuring the authorization database for granting access and rights to system resources. Each resource is assigned with different rights such as read, write and execute. Depending on the level of authorization (clearance) being set by the administrator, each authenticated entity can perform different actions on resources. A typical access control system has a policy for granting rights. These policies could vary from Discretionary Access Control (DAC), Mandatory Access Control (MAC) or a Multi-Level Security (MLS) model such as Role Based Access Control (RBAC) [44]. In DAC, the administrator is specifying the rights, while in MAC there are rules set by the system for assigning rights for subjects. Clearances are granted according to the role of the authenticated entity (Roles: course coordinator, lecturer or student in a university) in RBAC.

### 3.3 AUTHENTICATION AT IOT LAYERS

Authentication is the most critical security requirement in IoT for preserving the user identity and mitigating the threats as mentioned in the previous sections. With each IoT application, more hardware devices are introduced to be integrated to the IoT network. The authentication is the mechanism used to ensure the connectivity of those components to the existing ones. Authentication mechanisms involve cryptographic primitives for transmitting credentials securely. The strength of the scheme is entirely dependent on the crypto primitives being used. Though, developing a generic solution would be infeasible, as different layers attribute different requirements in IoT and the resources available for processing, memory and energy are diverse. Therefore, we will discuss the authentication requirements for each layer.

#### 3.3.1 Perception Layer

Perception layer includes all the hardware devices or the Machines to extract data from IoT environments. In most cases the authentication initiates as M2M connections. Thus, in this layer authentication could be conducted either as peer authentication or origin authentication [1]. In peer authentication, validation occurs between IoT routing peers, preliminary to routing information exchanging phase, while validating the route information by the connected peer IoT devices with its source is origin authentication. This method enhances the security in M2M communication. Though as mentioned previously, devices in Perception layer are inheriting inadequate resources for generating strong cryptographic primitives.

#### 3.3.1.1 Perception Nodes

These nodes are distributed across the IoT environment. Mostly, they are RFID tags and RFID readers / sensors, where few RFID tags are connected to a RFID reader. The connection establishment between RFID tags and the reader does not involve an authentication mechanism and would be vulnerable if the RFID tags can be cloned. An Identity Based Encryption (IBE) scheme was proposed by Chen [41] for establishing secure communication channel between RFID tags. Due to resource scarcity, an authentication protocol could be implemented using techniques such as Elliptic Curve Cryptography (ECC) based Diffie-Hellman (DH) key generation mechanism [1]. The generated keys, once they are transmitted to the two ends, could be used as the shared symmetric key for information transferring via the medium securely [44]. However, MiM attacks are still feasible and could be solved employing ephemeral DH method, by changing the ECC DH exponents for each connection establishment as a session key.

#### 3.3.1.2 Sensor Nodes and Gateways

Sensor nodes face similar security flaws as the perception nodes. Thus, deploying a proper authentication scheme could eliminate the possibility of being exposed to a very low level. However, sensors are much intelligent and resourceful than perception nodes. Hence, M2M authentication could be established as peer authentications and the origin authentication could be established via the sensor gateway. Similarly to the perception nodes, ECC based DH key exchange would be ideal for sensor nodes, where the ephemeral exponents are facilitated by the sensor gateway acting as a TTP. Identity validation of the sensor gateway should be conducted prior to any data transfer. Even though using certificates for identity determination is not practical, a similar parameter such as a serial number could be used when registering the sensor node in the IoT environment and all the identities are stored in the sensor gateway for validation. Sensor gateway should also possess a unique identity for mutual authentication to be established between the sensor node and the gateway. Moreover, countermeasures such as integrity violation detection (using Hashed Message Authentication Code – HMAC or Cipher Block Chaining MAC – CBC-MAC) and timestamps should be employed with the authentication protocols involved.

### 3.3.2 Network Layer

IoT network layer is integrated on top of the existing TCP/IP internet protocols. In this section we discuss the significance of the authentication for the components of the network layer.

#### 3.3.2.1 Mobile Communication

Security for mobile communication at network layer was not a critical necessity until the inception of IoT, as most of the mobile applications were relying on the inbuilt security protocols of the corresponding mobile technology (such as Global System for Mobile Communication - GSM, Wireless Code Division Multiple Access - WCDMA, High Speed Packet Access - HSPA or Long Term Evolution - LTE). With IoT, inbuilt authentication schemes are no longer foolproof, considering the potentiality for integrating technologies embedded in addition to the mobile technologies. Current security level and comprised resources (such as processor, memory and operating system) in mobile devices are adequate for designing tamper resistance authentication protocols at the network layer [5]. However, the existing key generation algorithms used in TCP/IP protocols for generating large and costly asymmetric keys (RSA, ElGamal or Paillier), are still not feasible to be used with mobile devices. Thus, generating unbreachable and lightweight keys would be the most challenging task in mobile communication.

Yao et al. [98] proposed a lightweight no-pairing Attribute Based Encryption (ABE) scheme based on ECC that is designed for handheld devices. Even though the improved mathematical complexity and linear relationship of the number of attributes with computational overhead are improving the robustness of the proposed ABE scheme, scalability of the scheme would be highly questionable with enormous amount of IoT devices. IBE schemes are also adoptable, if taking the identity parameter as the mobile

number or the user Social Security Number (SSN) for developing the authentication scheme integrating with ECC [41].

Current mobile devices include different biometric sensors for extracting biometrics such as fingerprint, iris, facial and voice imprints. Biometrics can be used as unique keys that could be used for authentication and can be employed with H2M authentication. As majority of the mobile devices at operation in an IoT environment are handled by a human user, the authentication design and the keys generation could be based on biometrics. The security of the biometrics schemes could be enhanced using several biometrics (multi-mode) integrated into multi-factor authentication schemes. These biometrically generated keys could be used as the signatures of each mobile entity for the verification of their identities and for conveying a secure session key among the communicating parties with proper encryption schemes. Additionally, authentication credentials should be checked for probable integrity violations in order to avoid MiM attacks.

#### 3.3.2.2 Cloud Computing

Clouds are the storage facility of IoT architecture and they are quite resourceful in terms of memory and processing. Thus, authentication should employ strong keys that are generated using public-key algorithms such as RSA or ElGamal, which are inviolable cryptographic primitives if the executing authentication mechanism are computationally feasible with the available resources. A symmetric key (AES, TDES, etc.) to be used in data transferring between the IoT devices and the cloud could be generated and shared among the entities that are engaged in a communication. Existing CAs could be used to validate the identity of the parties involved in communication via mutual authentication schemes for establishing the trust.

However, the main concern in cloud computing is the privacy of the user data. A strong authentication scheme does not ensure the misusing of information by the CSP. Thus, approaches such as blockchain and homomorphism should be considered for enhancing the privacy. The authentication schemes would be more secure in these schemes, as blockchain support pseudonymity (the nodes are identified from hashes or public keys – CA not required and simplify the authentication scheme) and the homomorphism facilitates additional layer of encryption to secure the communication [41].

Authorization techniques in clouds should be also be considered, as accessing the information in the clouds is vital for the IoT design. Existing access control mechanisms such as RBAC and MAC are not scalable and interoperable anymore. Thus, a novel method called Capability-Based Access Control (CapBAC), which uses capability based authority tokens to grant privileges to entities was proposed by Kouicem et al. [41].

#### 3.3.2.3 Internet

Even though authentication in most applications on internet is pursued by either SSL or IPSec protocols, IoT uses the DTLS as its communication protocol. However, the dependability of CAs for validating authentication parties still exists. Chinese CA WoSign was issuing certificates for false subjects in 2016, leaving an easier access to systems through wrongfully validated certificates for the attackers [2]. This happens when the trust of the system is centralized into a single entity. Thus, distributed access control schemes such as OpenPGP (widely used for email encryption) have formidable odds in succeeding in IoT infrastructure. Hokeun et al. in [2] introduces a locally centralized and globally distributed network architecture called Auth. Auth is to be deployed in edge devices for providing authorization services for locally registered entities, by storing their credentials and access policies in its database. Since the other instances of Auth are being distributed globally in the network, this maintains the trust relationships among them for granting authorizations for IoT devices acting as a gateway. Providing solution to the trust issue of CAs is the main concern for the Internet, as the security level in existing protocols is quite adequate.

### 3.3.3 Application Layer

Heterodyne nature of the IoT predicates the requirement for different approaches of access control mechanisms for different applications. Most of the existing application layer H2M authentication schemes are two factor authentication schemes, while the M2M ones are web based such as in SSL. The applicability and effectiveness of existing schemes is evaluated for each IoT application, since a generic solution is infeasible.

3.3.3.1 Smart Utilities – Smart Grids and Smart Metering

The intruders could perpetuate AMI interfaces stationed at every household or industrial plant, when using proper techniques. Once the access is granted to the hostile operators, potential outcomes could be devastating, as to the level of disrupting the energy flow of a local grid substation to overloading a nuclear reactor of a power station. Thus, access to the smart grids should only be granted to the local grid operator and the monitoring center, avoiding any interfacing through the AMI access points. Local grid operator authentication mechanism could be employed with a two-factor authentication scheme with a username, password and a RNG. A biometric scheme could be employable depending on the availability of biometric extraction devices. As the controlling access is given to the operator, an authorization scheme such as a RBAC should be employed, since a scalability concern does not exist with the limited number operators available for a smart grid. A M2M authentication interface is executed between the smart grid and the monitoring center for information access. Existing security protocols such as SSL could be used for authentication.

The access to AMI meter could be given to the residential consumer for the purpose of monitoring the statistics. This access could also be based on two-factor authentication or biometrics as the access is only given to read the data and not to manipulate it. Smart Grid has the ability to access the AMI meter through M2M authentication and should be secured with strong crypto primitives for preventing any MiM information extraction. Certificates should be issued to all the smart grids by a CA and the identities should be validated preferably via a mutual authentication scheme when establishing a grid to grid communication channel. A mechanism should be embedded with an authentication protocol for validating the AMI units for detecting possible tampering scenarios.

3.3.3.2 Consumer wearable IoT (WIoT) devices for healthcare and telemedicine

In a telemedicine system, the parties to grant access are the patients and their physicians only. Thus, the access should be limited. The authentication protocols should be always H2M when accessing the information, while M2M authentication operates when updating sensory information from wearable devices to the server. The access to the patient should be granted in a two-factor authentication scheme if a PC is being used for accessing. If the patient is using a mobile device for accessing the server, three-factor authentication scheme could be employed with integrating biometrics. Though, storing all the credentials including biometric templates at the authentication database would not be scalable with expanded healthcare services. Still authentication should be thorough since accessing PHRs are private and confidential. Cloud servers access to the physicians could be granted from a two-factor authentication scheme. The storing and accessing PHRs at the cloud could be secured with blockchain concept to counter the obvious privacy concerns with CSPs. An IBE scheme could be adopted to enhance the message transferring in the authentication protocol.

3.3.3.3 Intelligent Transportation and Logistics

Since the vehicles attribute high mobility, the connectivity of an established wireless links across vehicular entities may vary rapidly. Hence, the availability of a consecutive / fixed inter-link would be uncertain. Thus, dynamic handover mechanisms should be adopted between vehicular nodes for maintaining a consistent connection with communicating vehicular node. Hence, those handover based connections might require light-weight approach for authentication since they are highly dynamic.

Each vehicle should have an Identity based private key (embedded with its credentials – chassis no., registration no., manufacturer, model, etc.). But the keys should be generated from an IBE or ABE lightweight mechanism unlike public-key encryption schemes which require costly resources to generate. The authentication protocols are more likely to be M2M mechanisms, where the machines are the vehicles. Therefore, verifying the identity of each vehicular node engaged in communication is paramount to avoid malicious node invasions through a TTP based identity verification. ECC based ephemeral DH scheme could be employed for establishing a shard symmetric session key once the authentication phase is concluded after validating the vehicle identities. All V2V, V2I, V2G and Vehicle to Cloud (V2C) connections could be implemented in the same manner.

Additionally to the approaches discussed earlier, Software Defined Networks (SDN) and Blockchain concepts are highly recommended for ensuring the security requirements in the Application layer [1], [41].

#### 3.3.3.4 Smart Agriculture

As mentioned in the previous section regarding attacks, agriculture IoT devices intrinsically require a lightweight authentication protocol as they are vulnerable for external intervening and sparse resources with perception level nodes. With a lesser resourced platform, implementing a mutual-authentication scheme would be questionable. In [82], a logic based on Burrows-Abadi-Needham (BAN) modal logic was proposed and tested using Automated Validation Information Security Protocol Application (AVISPA) for verification, which was validated for MiM and replay attacks. However, a frequently changing session key usage is a paramount necessity to prevent perception level attacks. This session key establishment could be employed with a technique such as ephemeral DH or ECC for lesser resource utilization.

#### 3.3.3.5 IIoT

Most IIoT processes are M2M due to their automated platforms. Further, IIoT processes operations are continuous as their work cycles might extend to hours. With the amount of controlling data flowing through the communication channels, simultaneous authentication of each sensory node might alleviate the efficiency of the entire smart factory. Thus, a methodology for scheduled authentication scheme, which does not affect the industrial performance, should be established. However, the authentication at each sensory node could be evaded, as there might be hundreds of minor sensors connected to massive machines, which would be infeasible for authenticating each node frequently. Only the control information transfer of machines that is subject to authentication, as a single controlling command could last for hours continuously. These authentication phases could employ heavy cryptographic primitives as there is not any scarcity for computational resources.

#### 3.3.3.6 Smart Buildings, Environments and Cities

Designing a generic authentication protocol for smart cities is not practically feasible. Since the formation of this concept instantiate from the diminutive entity such as a smart home, inadequate security measures could compromise the privacy of users at any level of deployments [83]. However, this application could be visualized in the perspective of the three layers in IoT. Similar methods proposed for access control in perception layer could be adopted for the sensory system in the smart environments. Network layer accompanies all the internet integrated data connection and routing devices along with severs (clouds) additionally to the mobile devices. Mobile devices could use three factor authentication schemes incorporated with web based SSL or DTLS protocols, while cloud servers and routing nodes could be authenticated with cryptographically generated keys. Authentication protocols in smart cities are likely to change with the requirements and applications, as all other applications mentioned under this section are sub-applications of a smart city.

## 4 OTHER SECURITY FEATURES AND RELATED ISSUES

IoT systems have their own generalised features and requirements regardless of the diversified nature of its applications such as heterogeneity, scalability, Quality of Service (QoS)-aware, cost minimisation due to large scale deployment, self-management including self-configuration, self-adaptation, self-discovering, etc. The last but not least general feature/requirement on IoT system is to provide a secure environment to gain robustness to communication attacks, authentication, authorization, data transfer confidentiality, data/device integrity, privacy and to form a trusted secure environment [45]. IoT systems are fundamentally different from other transitional WSN systems [46] in many ways. 1) The diversity of the system has a much higher degree in terms of the type of the applications, the capabilities of the IoT devices and the attributes of the deployed environment, etc. 2) The holistic design of the system is mostly driven by the applications and it is essential to consider who are the users, what are the purposes and outcomes of the applications, etc. An IoT system is required to manage a large variety of devices, technologies and service environments since the system itself is highly heterogeneous, where the connected IoT devices or equipment can range from simple temperature sensors to high resolution smart cameras. The communication, computing and power capability of each device can be unique and distinguishing from others. These resource and interoperability constraints limit the feasibility for a standard security solution.

### 4.1 The Simplified Layer Structure

The traditional Open Systems Interconnection (OSI) has 7 layers: 1) The Physical Layer (Layer 1) is responsible for the transmission and reception of wire level data. 2) The Data Link Layer (Layer 2) is responsible for link establishment and termination, frame traffic control, sequencing, acknowledgement, error checking, and media access management. 3) The Network Layer (Layer 3) is implemented for routing of network traffic. 4) The Transport Layer (Layer 4) is responsible for message segmentation, acknowledgement, traffic control, and session multiplexing. 5) The Session Layer (Layer 5) is responsible for session establishment, maintenance and termination. 6) The Presentation Layer (Layer 6) is responsible for character code translation, data conversion, compression, and encryption. 7) The Application Layer (Layer 7) includes resource sharing, remote file access, remote printer access, network management, and electronic messaging (email). Since IoT systems normally have a large range of varieties from the choice of the hardware to the types of the applications, the traditional 7 network layers are simplified to 3 layers: perception layer, networking layer and application layer, as shown in Figure 1. The perception layer can be seen as the combination of the traditional physical layer and the MAC layer. It can include 2-D bar code labels and readers, RFID tags and reader-writers, camera, GPS, sensors, terminals, and sensor network. It is the foundation for the IoT system [47]. The networking layer is responsible for the data transmission and communication inside the system and with the outsider Internet. It should abstraction of the different underlying networks no matter it is wired, wireless or cellular. It can provide support for different communication modes including base station or access point based or Machine to Machine type based. The application layer is providing services to the end users and collecting data from different scenarios. IoT has high potentialities to implement smart and intelligent application for any using scenario in nearly every field. This is mainly because IoT can offer both 1) data collection through sensing over natural phenomena, medical parameters, or user habits and 2) data analysis and predict modelling for tailored services. Such applications will cover aspects such as personal, social, societal, medical, environmental, logistics, having a profound impact on the economy and society [45]. The perception layer and network layer together are considered as the foundation for the whole IoT system. These two layers together provide the backbone and the fundamental infrastructure of a IoT system. However, the architecture design and detailed implementation normally can only be confirmed after knowing the application layer design. Where the system will be deployed, what size of the field will be and what kind of data will be collected are all issues involved in the applications, but highly affect the decision making on the perception layer and network layer.

### 4.2 The Idea of Middleware

Researchers from academia and industry are exploring solutions to enhance the development of IoT from three main perspectives: scientific theory, engineering design, and the user experience [48]. These activities can enrich the technologies for IoT, but also increase the complexities, when implementing such a system in real world. For this reason, the concept of IoT middleware has been introduced and many systems are already available [49, 50, 51, 52, 53]. However, when defining the formal definition for IoT middleware, researchers have different understandings. In some circumstance, IoT middleware is equivalent to IoT Operating System (OS). In general, middleware can simplify and accelerate a development process by integrating heterogeneous computing and communications devices, and supporting interoperability within the diverse applications and services [54]. Most existing implementations for middleware are designed for WSN and not for service oriented IoT system. Though, certain IoT-Specific middleware exist [55, 56]. In reality, middleware is often used to bridge the design gap between application layer and the lower infrastructure layers. The requirements for middleware service for the IoT can be categorised into functional and non-functional groups. Functional requirements capture the services or functions such as abstractions and resource management [57]. Non-functional requirements capture QoS support or performance issues such as energy efficiency and security [58].

The Internet of Everything (IoE) aims to bring the objects, buildings, roads and cities all connected and also make the platform to be accessible. This feature will significantly increase the vulnerabilities of the system and the inherent complexity of the IoT further complicates the design and deployment of efficient, interoperable, and scalable security mechanisms. It has been clear stated that all the typical security issues (authentication, privacy, nonrepudiation, availability, confidentiality, integrity) exist on all the layers and the entire function box to a certain degree. However, when implementing security solutions, different layers of different systems will have specialised priorities.

An essential task of the middleware is to provide secured data transmission between the upper and lower layers. For inner system communication, it should guarantee that the data passed to the application layer from the infrastructure is safe and reliable to use — integrity. Integrity in this scenario involves maintaining the consistency, accuracy, and trustworthiness of data over the transmission. The other way around, the middleware should also ensure that the control comments and queries from the applications/end users are verified and it is harmless for the system to take actions — non-repudiation. Non-repudiation feature ensure that the users cannot deny the authenticity of their signature for their documents and footprints for their activities. In addition, the middleware must protect the data transmission and information exchange between the upper and lower layers from illegal external access by any arbitrary user. The data must not be disclosed to any unauthorised entities — confidentiality.

### 4.3 Cross-Layer Security Problem

It has been frequently argued that although layered architectures have been a great success for wired networks, they are not always the best choice for wireless networks. To address this problem, a concept of cross-layer design is proposed and it is becoming popular. This concept is based on an architecture where different layers can exchange information in order to improve the overall network performance. Substantial amount of work has been carried out on state of the art cross-layer protocols in the literature recently [59]. Security can be considered as one of the most critical QoS features in IoT systems. Wireless broadcast communication is suffering security risks more than others while multi-hop wireless communication is in a worse situation, since there is no centralised trusted authority to distribute a public key in a multi-hop network due to the nature of its distribution. Current proposed security approaches may be effective to a particular security issue in a specific layer. However, there still exists a strong need for a comprehensive mechanism to prevent security problems in all layers [60]. Security issues like availability need to be address not only at each layer, but a good cross layer design and communication is encouraged. IoT systems are generally large and complex systems with many interconnections and dependencies, such as in smart cities [61].

If the availability of any of the three layers (perception, network and application) fails, the availability of the whole system collapses. The lower layer infrastructure must protect itself from malicious behavioural patterns and harmful control from unauthorised users. Application layer should be available for all authorised users continuously without any service overloading type interruption from unauthorised users.

### 4.4 Privacy

As the new European General Data Protection Regulation (GDPR)[2] has become enforceable on 25 May 2018, protecting user data and securing user privacy are urgent and predominant to be solved for any IoT application. Users' data cannot be captured nor used without their awareness. Privacy has the highest priority for all existing and future application development, including IoT systems. User identities must not be identifiable nor traceable. Under the new legislation, data processing must involve:

1) Lawful, fair and transparent processing — emphasising transparency for data subjects.

2) Purpose limitation — having a lawful and legitimate purpose for processing the information in the first place.

3) Data minimisation — making sure data is adequate, relevant and limited, and organisations are sufficiently capturing the minimum amount of data needed to fulfil the specified purpose.

4) Accurate and up-to-date processing — requiring data controllers to make sure information remains accurate, valid and fit for purpose.

5) Limitation of storage in a form that permits identification — discouraging unnecessary data redundancy and replication

6) Confidential and secure — protecting the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security)

7) Accountability and liability — the demonstrating compliance. As a well-known statement in security, there are security issues at all perception, network and application layers.

Some other security problem can be addressed effectively and efficiently on a certain layer level, such as in implementing privacy component on application layer. In a healthcare system, patients should be totally aware who is collecting and using their data. They also should have the controls over the data and who they want to share with, how and where their data is being used. The applications should provide services and interface to allow users to manage their data. Users must have tools that allow them to retain their anonymity in this super-connected world. The same scenario can be applied to systems such as smart home, smart transportation, etc. IoT applications may collect users' personal information and data from their daily activities. Many people would consider that data or information predicted from the data as private. Exposure of this information could have an unwanted or negative impact to their life. The use of the IoT system should not cause problems of privacy leaking. Any IoT applications which do not meet with these privacy requirements could be prohibited by law. The IoT system must seriously consider the implementation of privacy by the 7 data protection principles, providing user-centric support for security and privacy from its very own foundations [62].

### 4.5 Risk Mitigation

Mitigating the risk of an intrusion attempt or attack against an IoT device is not an easy thing to do. Having a higher degree of security protection at every level will discourage the attacker to pursue his goals further, by cause of the amount of effort and time needed versus benefits. Mitigation needs to start with prevention, by involving every actor in the market, from manufacturers to consumers and

[2] https://www.eugdpr.org/

lawmakers, and make them understand the impact of the IoT security threats in a connected world. Another way to mitigate risk is to keep abreast of the times by improving and innovating, from the ground up, and by finding new methods and designs to outgrow the shortcomings of the market.

## 5 DISCUSSION

Authentication for IoT is a paramount necessity for securing and ensuring privacy of users, simply due to the fact that an impregnable access control scheme would be impervious for any attack vector originating outside of the considered trust domain, as explained in the previous sections of this book chapter. Authentication schemes in IoT applications are generally implemented in the software level, in which it exposes the hardware and design vulnerabilities that are unintentional [84]. This fact constitutes the requirement of a holistic approach for securing access to the systems via employing impregnable authentication schemes. However, developing a generic authentication scheme to counter all possible attack scenarios would be improbable and an arduous attempt due to the heterogeneity of the IoT paradigm. A layered approach which concatenates the optimum authentication schemes applicable at differentiated levels to formalize a holistic trust domain is a desideratum.

For perception level entities, IBE or ECC would be ideal authentication schemes to generate commendable cryptographic credentials with available resources. The mobile entities, where the actual users are interfacing to IoT systems are storing personalized credentials such as photos, medical stats, access to CCTV systems, GPS location (GPS), daily routines, financial stats, banking credentials, emergency service status and online account statistics, are emphasizing the requisite for privacy preservation at this level. As proposed in section 3.3.2.1, adopting IBE, ABE, ECC or biometric based mechanisms should be ensuring security. Novel mechanisms such as CapBAC could be employed to launch a scalable access control scheme for cloud computing platforms for IoT applications. However, potential for deploying edge computing paradigms in the edge of the network indemnifies the cloud computing services from external direct access, as the access controlling would be migrated to the edge along with the service platform. The internet technologies of IoT enabled systems are secured than the perception level and mobile level entities with the deployed protocols such as DTLS, SSL and IPSec. Due to the dependency of a CA or TTP for employing such strong and secure protocols, the future of Internet security enhancements would be focused on developing distributed access control schemes to eliminate the single point of failure. Each IoT application composes different devices and systems to accomplish the intended outcome which attributes diverse protocols in hardware and software. Thus, the authentication schemes should be application specific and context aware of resource constraints associated with the diversified deployments. As the privacy is the main concern on IoT to be ensured through impregnable access control schemes, the GDPR initiative is a timely solution established to constrict the IoT service providers (both software and hardware) from developed and marketing products with vulnerabilities.

Current researches have focused on developing novel methods for authentication in IoT domain. We are briefly introducing few of these recent approaches to demonstrate the state of the art technologies.

In [88], Ning et al. has proposed an aggregated proof based hierarchical authentication (APHA) scheme to be deployed on existing Unit IoT and Ubiquitous IoT (U2IoT) architecture. Their scheme employs two cryptographic primitives; homomorphic functions and Chebyshev polynomials. The proposed scheme has been verified formally using Burrows-Abadi-Needham (BAN) logic. However, the scalability of the scheme with the extent of multiple units has not been verified with a physical prototype.

There are various initiatives on Physical Unclonable Functions (PUF) to be used for IoT device authentication. A PUF is an expression of an inherent and unclonable instance-specific unique feature of a physical object which serves as a biometric for non-human entities, such as IoT devices [91]. Hao et al. are proposing a Physical Layer (PHY) End to End (E2E) authentication scheme which generates an IBE based PHY-ID which acts as a PUF with unclonable PHY features RF Carrier Frequency Offset (CFO) and In-phase/Quadrature-phase Imbalance (IQI) extracted from collaborative nodes in a Device to Device (D2D) IoT deployment [89]. This mechanism is ideal for perception level nodes to be impervious to impersonation or malicious node injection attacks, as it is using physical measurements which are unique for each entity and for its location of operation in generating an identity for devices. Though, the proposed scheme relies on a TTP called Key Generation Centre (KGC). KGC generates the asymmetric key credentials for the nodes in its contact. The reachability of a certain KGC is limited due to the low power D2D connectivity. Thus, multiple KGCs deployed to accomplish the coverage should be managed with a centralized control entity. This enables the attack vectors on decentralized KGC entities. Moreover, the reliance on CFO and IQI features require the nodes to be stationary. This would be an issue considering most IoT devices are mobile and their RF based characteristics are varying in a timely manner. Aman et al. proposed a PUF based authentication protocol for scenarios when an IoT device is connecting with a server and a D2D connectivity focused on its applicability in vehicular networks. Authentication is based on a Challenge Response Pair (CRP), where the outcome of the CRP is correlated with the physical microscopic structure of the IoT device, which emphasizes its unique PUF attributes with the inherent variability of the fabrication process in Integrated Circuits (ICs). The proposed protocol was analysed using Mao and Boyd logic, while Finite State Machine (FSM) and reachability analysis techniques have been adopted for formal verification. Even though the performance of the protocol has been analysed in terms of computational complexity, communication overhead and storage requirement, its scalability with simultaneous multiple IoT device connections to the server have not been addressed. However, this approach would be a feasible solution for V2E applications as the PUF could be successfully integrated with vehicles.

A human gait pattern based on the biometric extraction scheme WifiU has been proposed in [90] as a case study that uses Channel State Information (CSI) of the received Wi-Fi signals for determining the gait pattern of the person carrying the transmitter. The gait patterns are becoming a novel biometric mode and this solution is a cost effective approach which does not employ any floor sensors or human wearables. Though, the applicability of WifiU for IoT devices raises concerns over scalability, accuracy of the gait pattern extraction from CSI, reliability of CSI measurement and Wi-Fi interference. Chauhan et al. in [92] proposes a Recurrent Neural Network (RNN) based on human breath print authentication system for mobile, wearable and IoT platforms employing a derived breath print as a biometric through acoustic analysis. Even though this approach depicts a viable biometric solution for human interfacing IoT applications, the breath print extraction would be dependent on the health, climatic circumstances and physical stability of the user.

If the proposed authentication schemes are not fully holistically applicable for IoT deployments, optimum solutions at different layers and specific applications could be aggregated to form an impregnable access control system, where the interconnectivity among them should be maintained by a decentralized trust domain managers. However, the access control mechanism optimum for each application should be investigated for each case in order to ensure robustness.

## 6 FUTURE RESEARCH DIRECTIONS

This section proposes several new research approaches and directions that could have a high impact for the future of the IoT security.

### 6.1 Blockchain

The blockchain is a distributed database of online records. Typically used in financial transactions for the Bitcoin cryptocurrency, the peer-to-peer blockchain technology records transactions without exception, in exchange to form an online ledger system. Blockchain technologies are immutable, transparent, trustworthy, fast, decentralised and autonomic, providing solutions that can be public, consortium or private. Due to the success of Bitcoin, people now start to apply blockchain technologies in many other fields, such as financial market, supply chain, voting, medical treatment and security for IoT [63]. There are expectations that blockchain will revolutionise industry and commerce and drive economic change on a global scale [64].

Blockchain technology leads to the creation of secure mesh networks, where IoT devices will interconnect while avoiding threats such as impersonation or device spoofing. As more legitimate nodes register on the blockchain network, devices will identify and authenticate each other without a need for central brokers and certification authorities. The network will scale to support more and more devices without the need for additional resources [65].

Smart contracts open the way to defining a new concept, a decentralized autonomous organization (DAO), sometimes labelled as a decentralized autonomous corporation (DAC), an organization that runs through rules maintained on a blockchain. The legal status of this new brand of business organization is rather seen as a general partnership, meaning that its participants could bear unlimited legal liability. Ethereum blockchain, for example, is a public blockchain network optimized for smart contracts that use its cryptocurrency, called Ether (ETH). There is a huge interest in Ethereum, as a blockchain technology for the future. In 2017 Enterprise Ethereum Alliance is formed and already counting close to 100 members, like Samsung, Microsoft, J.P.Morgan, Toyota, ING, Consensys, BP, Accenture and many others. Etherum has become the second highest traded cryptocurrency in 2017, after Bitcoin, with a volume of transactions for over half of million euros in 24h.

As with each disruptive concept that turns into an effective offering, the blockchain model is not perfect and has its flaws and shortcomings. Scalability is one of the main issues, considering the tendency towards centralization with a growing blockchain. As the blockchain grows, the nodes in the network require more storage, bandwidth, and computational power to be able to process a block, which leads to only a handful of the nodes being able to process a block. Computing power and processing time is another challenge, as the IoT ecosystem is very diverse and not every device will be able to compute the same encryption algorithms at the desired speed. Storage of a continuously increasing ledger database on a broad range of smart devices with small storage capabilities, such as sensors, is yet another hurdle. The lack of skilled people to understand and develop the IoT-blockchain technologies together is also a challenge. The lack of laws and a compliance code to follow by the manufacturers and service providers is not helping both the IoT and blockchain to take off as expected.

IOTA solves some problems that the blockchain does not. One of them is centralization of control. As history shows, small miners create big groups to reduce the variation of the reward. This activity leads to concentration of power, computational and political, in possession of just a handful of pool operators and gives them the ability to apply a broad spectrum of policies, like filtering on or postponing certain transactions.

### 6.2 5G

For the first time in history LTE has brought the entire mobile industry to a single technology footprint resulting in unprecedented economies of scale. The converged footprint of LTE has made it an attractive technology baseline for several segments that had traditionally operated outside the commercial cellular domain. There is a growing demand for a more versatile M2M platform. The challenge for industrial deployment of IoT is the lack of convergence across the M2M architecture design that has not materialised yet. It is expected that LTE will remain as the baseline technology for wide area broadband coverage also in the 5G area. The realisation of 5G network is affecting many IoT protocols' initial design, especially at perception and network layers [66]. Mobile operators now aim to create a blend of pre-existing technologies covering 2G, 3G, 4G, WiFi and others to allow higher coverage and availability, and higher network density in terms of cells and devices with the key differentiator being greater connectivity as an enabler for M2M services [67]. 3GPP standard/5G based backhaul has become a popular solution for connectivity problem in IoT systems. Munoz et al. indicates that the next generation of mobile networks (5G), will need not only to develop new radio interfaces or waveforms to cope with the expected traffic growth but also to integrate heterogeneous networks from End to End (E2E) with distributed cloud resources to deliver E2E IoT and mobile services [68]. Fantacci et al. has provided a backhaul solution through mobile networks for smart building applications [69]. The proposed network architecture will improve services for users and also will offer new opportunities for both service providers and network operators. As 5G has becoming available and being adopted as the main backhaul infrastructure for IoT system, it will play a huge role in IoT perception and networking layers [70]. 5G has moved the focus to user centric service from network centric service unlike 4G and 3G. With massive multiple-input and multiple-output (MIMO) technologies deployed in 5G, network selection and rapid handovers are becoming essential in terms of supporting QoS and Quality of user Experience (QoE) aware services [71]. The handover between different network interfaces should be authenticated and the information exchange during the handover should be protected and private. Currently, SDN is considered as the main stream for a higher efficiency through its centralised control capability in 5G communication process [72]. With SDN, the control logic is removed from the underlying infrastructures to a management platform. Software and policies can be implemented on the central SDN controller to provide consistent and efficient management over the whole 5G network. One advanced and beneficial feature offered by SDN is that it can separate the control plane and data source by abstract, the control logic from the underlying switches and routers to the centralised SDN controller [73]. To address the Machine Type Communication (MTC) in IoT systems based on 5G network, several approaches are available [74], [75]:

1) A higher level of security for devices is achievable by utilising new security mechanisms being embedded with Subscriber Identity Module (SIM).

2) It is recommended to implement and employ physical-layer security adopting RF fingerprinting.

3) Using asymmetric security schemes to transfer the burden of required computations to the network domain or gateways with high computing capabilities.

### 6.3 Fog and Edge Computing

Although powerful, the cloud model is not the best choice for environments where internet connectivity is limited or operations are time-critical. In scenarios such as patient care, milliseconds have fatal consequences. As well in the vehicle to vehicle communications, the prevention of collisions and accidents relies on the low latency of the responses. Cloud computing is not consistently viable for many IoT applications, and so, it is replaced by the fog computing. Fog computing, also known as fogging, is a decentralized computing infrastructure in which the data, compute, storage and applications split in an efficient way between the data source and the cloud.

Fog computing extends the cloud computing and services alike, to the edge of the network, by bringing the advantages and the power of the cloud to where the data arise initially. The main goal of fogging is to improve efficiency and also to reduce the quantity of data that moves to the cloud for processing, analysis, and storage. In fogging, data processing takes place in a router, gateway or data hub on a smart device, which sends it further to sources for processing and return transmission, therefore reducing the bandwidth payload to the cloud.

The back-and-forth communication between IoT devices and the cloud can negatively affect the overall performance and security of the IoT asset. The distributed approach of fogging addresses the problem of the high amount of data coming from smart sensors and IoT devices, which would be costly and time-consuming to send to the cloud each time. Among other benefits, the fog computing offers better security by protecting the fog nodes with the same policy, controls, and procedures used in other parts of the IT environment and by using the same physical safety and cyber security solutions [76]. Fog networking complements the cloud computing and allows for short-term analytics at the edge while the cloud performs resource-intensive, longer-term analytics. Computation moves even closer to the edge and becomes deeply-rooted in the very same devices that created the data initially, and so, generating even greater possibilities for M2M intelligence and interactions.

The movement of computation from the fog to the actual device opens the path to edge computing. That is a distributed architecture in which the processing of client data takes place at the outer edge of the network, in the proximity of the originating source. The mobile computing, the low cost of computer components and the absolute quantity of IoT devices drive the move towards edge computing. Time-sensitive data is processed at the point of origin by an intelligent and resource-capable device or sent to a broker server located in close geographical proximity to the client. Less time-sensitive data travels to the cloud for historical analysis, big data analytics, and long-term storage. One of the greatest benefits of edge computing is that it removes network bottlenecks by improving time to action and response time down to milliseconds, while also conserving network resources.

The edge computing concept is not without its flaws though. Edge computing raises a high amount of security, licensing and configuration challenges and concerns. The vulnerability to some attack vectors like malware infections and security exploits increases because of the nature of the distributed architecture. Smart clients can have hidden licensing costs, where the base version of an edge client might initially have a low price, additional functionalities could be licensed separately and drive the price up. Also, decentralized and poor device management leads to causing configuration drift by the administrators. They can inadvertently create security holes by not consistently updating the firmware or by failing to change the default password on each edge device [77].

### 6.4 Quantum security, AI, and Predictive Data Analytics

With the technological advancements of quantum computing, Artificial Intelligence (AI), and cognitive systems, and with the continuous development and mass adoption of IoT ecosystem, the current security practices and methodologies will become a part of the past. Quantum computing, not only that it can break through any form of security that is known to human kind, but it can also offer the solution to finding the formula for tight security. IoT will vastly benefit from these technology advancements, especially from the quantum mechanics science on a microchip. Further research is recommended, once the technology matures and evolves, to discover how the security of the future impacts on the things around and especially on the Internet of Things ecosystem.

### 6.5 Network Slicing

Network slicing is the concept of slicing a physical network into several logical planes to facilitate the various IoT services to customize their differentiated on-demand services with the same physical network [93]. The main aim of this paradigm is to reinforce different service requirements such as latency, bandwidth and reliability of heterogeneous IoT applications to utilize the resources such as storage, computing and bandwidth of the IoT device platforms [94]. The complexity of the IoT service integration with core network resources could be alleviated using a standardized network slicing mechanism as proposed by the Next Generation Mobile Network (NGMN). A typical network slicing process could be described under three layers, namely service instance layer, network slice instance layer and resource layer which follows the principles automation, isolation, customization, elasticity, programmability, end-to-end and hierarchical abstraction [96].

The evolvement of network slicing concept has reached the depths of 5G Information Centric Networking (ICN) model, which consist of five functional planes (FPs), namely; FP1 - service business plane, FP2 - service orchestration and management plane, FP3 - IP/ICN orchestrator plane, FP4 - domain service orchestration and management plane and FP5 - infrastructure plane. FP1 interfaces with external 5G users in providing various service APIs which realizes the objective and relevant services to accomplish that objective with inputs such as service type, demand patterns, Service Level Agreements (SLA) / QoS/ QoE requirements. The service requests forwarded by FP1 are communicated to the FP3 as service requirements by FP2. The FP3 interfaces with a domain controller to virtualize compute, storage and network resources to meet the service requirements conveyed from FP2. FP4 supports the management of IP and ICN services belonging to different technological domains such as 4G/ 5G RAN, Multi-Protocol Label Switching (MPLS) and edge technologies, while FP5 enables the service rules in end-to-end manner.

The entities operating in network slicing infrastructure, such as network slice manager and host platforms are attributing the vulnerabilities exploitable by impersonation attacks, DoS, SCA attacks and the interoperability of different security protocols and policies [95]. An IoT user may access different slices depending on the requirements and the intended outcomes. Thus, the access granting control for different slices is a critical juncture in the perspective of security. The plausibility for isolating the slices for constricting the deliberate hacking attempts at resources operating at each plane should be focused. Due to the facts that a network slice is a composite of the actual physical infrastructure and the processes should be dynamic, adaptive and flexible for servicing the intended functions, the assurance of user confidentiality, privacy, integrity and availability are challenging. However, authentication is the most effective mechanism to be used for enhancing the robustness of the network slices towards attacks. Among the 5G Security –as-a-Service (SaaS) concepts, micro-segmentation, deception of the attacker and AI deployments for monitoring, attack detection and remediation are emerging initiatives for securing network slices [97].

## 7 CONCLUSIONS

IoT technology is the most discussed paradigm in the research community these days. Its potential to connect all the devices in the world and to create a large information system that would offer services to improve the quality of human beings exponentially has made the concept much popular. The integration of various technologies and devices with different architectures are creating interoperability issues with the components in the IoT architecture. These issues and the highly diversified types of services are creating security concerns which disperse into all three layer of IoT architecture: Perception, Network and Application. Hence, the security measures to be taken should be developed while analysing the threats and vulnerabilities at each layer.

Mitigating risks associated with security breaches are possible, if security receives consideration from early product planning and design, and if some basic prevention mechanisms are in place. Enactment and standardization will simplify the manufacturing and development processes, give the market an incentive for mass-adoption and also increase the security posture of IoT products and services. Security will have to be inbuilt so that IoT can withstand a chance against the threats that technological advancements will bring along.

## REFERENCES


[1] F. Alaba, M. Othman, I. Hashem and F. Alotaibi, “Internet of Things security: A survey”, Journal of Network and Computer Applications, 88, pp.10-28, 2017.

[2] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in IT Professional, vol. 19, no. 5, pp. 27-33, 2017. doi: 10.1109/MITP.2017.3680960

[3] Jurcut, A., Coffey, T., Dojen, R. and Gyorodi, R., “Analysis of a key-establishment security protocol”, Journal of Computer Science and Control Systems, Vol. 2008, ISSN 1844-6043, pp. 42-47, 2008.

[4] Jurcut, A.D., Coffey, T., Dojen, R., “On the Prevention and Detection of Replay Attacks using a Logic-based Verification Tool**”,** In: Computer Networks, Series: Communications in Computer and Information Science, Springer International Publishing Switzerland, Volume 431, ISBN: 978-3-319-07940-0, pp. 128-137, June , 2014, DOI: 10.1007/978-3-319-07941-7_13

[5] Jurcut, A.D., Liyanage, M., Chen J., Gyorodi C., He, J., “On the Security Verification of a Short Message Service Protocol”, 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, April 2018. DOI: 10.1109/WCNC.2018.8377349

[6] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32-37, DOI: 10.1109/I-SMAC.2017.8058363.

[7] Vladimir Pasca, Anca Jurcut, Reiner Dojen, Tom Coffey. “Determining a Parallel Session Attack on a Key Distribution Protocol using a Model Checker“, ACM Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia (MoMM ’08), ISBN: 978-1-60558-269-6, pp. 150-15,5 Linz, Austria, 2008, DOI: 10.1145/1497185.1497218

[8] Jurcut, A.D., Coffey, T., Dojen, R., "A Novel Security Protocol Attack Detection Logic with Unique Fault Discovery Capability for Freshness Attacks and Interleaving Session Attacks", IEEE Transactions on Dependable and Secure Computing, July 2017.

[9] Liyanage, M., Braeken, An., Jurcut, A.D., Ylianttila, M.,Gurtov. A., “Secure Communication Channel Architecture for Software Defined Mobile Networks”, *Journal of Computer Networks*114:32-50 , *Elsevier*, February 2017 DOI: 10.1016/j.comnet.2017.01.007

[10] A Jurcut, T Coffey, R Dojen, “Design requirements to counter parallel session attacks in security protocols”, 12th IEEE Annual Conference on Privacy, Security and Trust (PST’14), ISBN: 978-1-4799-3502-4, pp. 298 – 305, Toronto, Canada , July 2014, DOI: 10.1109/PST.2014.6890952.

[11] Jurcut, A.D., Coffey, T. , Dojen, R., “Design Guidelines for Security Protocols to Prevent Replay & Parallel Session Attacks**”,** *Journal of Computers & Security, Elsevier*, Volume 45, pp. 255–273, September 2014**,** DOI: 10.1016/j.cose.2014.05.010

[12] Jurcut, A.D., Coffey, T. , Dojen, R., **“**Symmetry in Security Protocol Cryptographic Messages – A Serious Weakness Exploitable by Parallel Session Attacks”, 7th IEEE International Conference on Availability, Reliability and Security (ARES’12), ISBN: 978-1-4673-2244-7, Prague, Czech Republic, 20-24 August 2012, DOI: 10.1109/ARES.2012.39

[13] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D., 2014. Security of the Internet of Things: perspectives and challenges. Wirel. Netw. 20 (8), 2481–2501.

[14] K. Zhao and L. Ge, “A survey on the internet of things security,” in Computational Intelligence and Security (CIS), 2013 9th International Conference on, pp. 663–667, IEEE, 2013

[15] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, “Security and privacy aspects of low-cost radio frequency identification systems,” in Security in pervasive computing, pp. 201–212, Springer, 2004.

[16] D. Henrici and P. M¨uller, “Tackling security and privacy issues in radio frequency identification devices,” in International Conference on Pervasive Computing, pp. 219–224, Springer, 2004.

[17] E. B. Kavun and T. Yalcin, “A lightweight implementation of keccak hash function for radio-frequency identification applications,” in International Workshop on Radio Frequency Identification: Security and Privacy Issues, pp. 258–269, Springer, 2010.
[18] Zhang, Y., Shen, Y., Wang, H., Yong, J., Jiang, X., 2015. On secure wireless Communications for IoT Under Eavesdropper Collusion. IEEE Trans. Autom. Sci. Eng. 13 (3), 1281–1293.
[19] Massis, B., 2016. The Internet of Things and its impact on the library. New Libr. World 117 (3/4), 289–292.
[20] Liu, Y., Cheng, C., Gu, T., Jiang, T., Member, S., Li, X., 2016. Scheme Smart Grid 16 (3), 836–842.
[21] https://blog.smartbear.com/iot-2/how-to-protect-iot-gateways-from-security-vulnerabilities/ (Online; accessed on 04 May 2018)
[22] Horrow, S., Anjali, S., 2012. Identity management framework for cloud based Internet ofThings. In: Proceedings of the First International Conference on Security of Internet of Things, SecurIT’ 12 , 200‑203.
[23] X. Lin et al., “TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving,” IEEE Trans. Wireless Commun., vol. 7, no. 12, 2008, pp. 4987–98.
[24] X. Lin and X. Li, “Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks,” IEEE Trans. Vehic. Tech., vol. 62, no. 7, 2013, pp. 3339–48.
[25] J. Zhou et al., “4S: A Secure and Privacy-Preserving Key Management Scheme for Cloud-Assisted Wireless Body Area Network in m-Healthcare Social Networks,“ Info. Sciences, vol. 314, 2015, pp. 255–76.
[26] J. Sen, “Privacy Preservation Technologies in Internet of Things,” Proc. Int’l. Conf. Emerging Trends in Mathematics, Technology, and Management, 2011.
[27] J. Zhou et al., “4S: A Secure and Privacy-Preserving Key Management Scheme for Cloud-Assisted Wireless Body Area Network in m-Healthcare Social Networks,“ Info. Sciences, vol. 314, 2015, pp. 255–76.
[28] J. Zhou et al., “Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs,” IEEE Trans. Info. Forensics and Security, vol. 10, no. 6, 2015 , pp. 1299–314.
[29] R. Roman et al., “Key Management Systems for Sensor Networks in the Context of the Internet of Things,” Computer & Electrical Engineering, vol. 37, no. 2, 2011, pp. 147–59.
[30] J. Zhou et al., “TR-MABE: White-Box Traceable and Revocable Multi-Authority Attribute-Based Encryption and Its Applications to Multi-Level Privacy-Preserving e-Heathcare Cloud Computing Systems,“ IEEE INFOCOM 2015.
[31] R. Lu et al., “Pi: A Practical Incentive Protocol for Delay Tolerant Networks,“ IEEE Trans. Wireless Commun., vol. 9, no. 4, Apr. 2010, pp. 1483–92.
[32] P. Paillier, “Public Key Cryptosystems Based on Composite Degree Residuosity Classes,” Eurocrypt ‘99, pp. 223–38.
[33] J. Groth and A. Sahiai, “Efficient Noninteractive Proof Systems for Bilinear Groups,“ Advances in Cryptology®EUROCRYPT 2008, Springer Berlin, 2008., pp. 415–32.
[34] Akhunzada, A., Gani, A., Anuar, N.B., Abdelaziz, A., Khan, M.K., Hayat, A., Khan, S.U., 2016. Secure and dependable software defined networks. J. Netw. Comput. Appl. 61, 199–221.
[35] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[36] Mendez, Diego M., Ioannis Papapanagiotou, and Baijian Yang. "Internet of things: Survey on security and privacy." arXiv preprint arXiv:1707.01879 (2017).
[37] Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications 88 (2017): 10-28.

[38] O. Garcia-Morchon, R. Hummen, S. Kumar, R. Struik, and S. Keoh, “Security considerations in the ip-based internet of things, draft-garciacore-security-04,” 2012.
[39] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty security considerations for cloud-supported internet of things,” 2015.
[40] Bekara, C., Security issues and challenges for the IoT-based smart grid, in Procedia Comput. Sci. 34, 532–537, 2014.
[41] D. Kouicem, A. Bouabdallah and H. Lakhlef, “Internet of things security: A top-down survey. Journal of Computer Networks, 2018.
[42] Desai, Drushti, and Hardik Upadhyay. "Security and Privacy Consideration for Internet of Things in Smart Home Environments." *International Journal of Engineering Research and Development* 10, no. 11 (2014): 73-83.
[43] Kumar, J. Sathish, and Dhiren R. Patel. "A survey on internet of things: Security and privacy issues." *International Journal of Computer Applications* 90, no. 11 (2014).
[44] M. Stamp, Information security, 2nd ed. Hoboken, N.J.: Wiley, 2011, pp. 227-278.
[45] E. Borgia, “The internet of things vision: Key features, applications and open issues,” Computer Communications, vol. 54, pp. 1 – 31, 2014.
[46] L. Xu, R. Collier, and G. M. P. 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, vol. 4, pp. 1229–1249, Oct 2017.
[47] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of internet of things,” in 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5, pp. V5–484–V5–487, Aug 2010.
[48] M. A. Feki, F. Kawsar, M. Boussard, and L. Trappeniers, “The internet of things: The next technological revolution,” Computer, vol. 46, pp. 24–25, Feb 2013.
[49] “Contiki,” Accessed: 2018-05-17. http://www.contiki-os.org/.
[50] “Brillo,” Accessed: 2018-05-17. https://developers.google.com/brillo/.
[51] “Tinyos,” Accessed: 2018-05-17. http://www.tinyos.net/.
[52] “Openwsn,” Accessed: 2018-05-17. http://openwsn.atlassian.net.
[53] “Riot,” Accessed: 2018-05-17. http://www.riot-os.org/.
[54] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, “Middleware for internet of things: A survey,” IEEE Internet of Things Journal, vol. 3, pp. 70–95, Feb 2016.
[55] C. Perera, P. P. Jayaraman, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Mosden: An internet of things middleware for resource constrained mobile devices,” in 47th Hawaii International Conference on System Sciences, pp. 1053–1062, Jan 2014.
[56] H. Zhou, The Internet of Things in the Cloud: A Middleware Perspective. Boca Raton, FL, USA: CRC Press, Inc., 1st ed., 2012.
[57] L. Xu, D. Lillis, G. M. O’Hare, and R. W. Collier, “A user configurable metric for clustering in wireless sensor networks.,” in SENSORNETS, pp. 221–226, 2014.
[58] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, “Iot middleware: A survey on issues and enabling technologies,” IEEE Internet of Things Journal, vol. 4, pp. 1–20, Feb 2017.
[59] V. Srivastava and M. Motani, “Cross-layer design: a survey and the road ahead,” IEEE Communications Magazine, vol. 43, pp. 112–119, Dec 2005.
[60] Q. Zhang and Y. Q. Zhang, “Cross-layer design for qos support in multihop wireless networks,” Proceedings of the IEEE, vol. 96, pp. 64–76, Jan 2008.
[61] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” IEEE Internet of Things Journal, vol. 1, pp. 22–32, Feb 2014.

[62] 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, no. 10, pp. 2266 – 2279, 2013. Towards a Science of Cyber Security Security and Identity Architecture for the Future Internet.
[63] I. C. Lin and T. C. Liao, “A survey of blockchain security issues and challenges,” I. J. Network Security, vol. 19, pp. 653–659, 2017.
[64] S. Underwood, “Blockchain beyond bitcoin,” Commun. ACM, vol. 59, pp. 15–17, Oct. 2016.
[65] "How blockchain can change the future of IoT," 20 Novemver 2016. [Online]. Available: https://venturebeat.com/2016/11/20/how-blockchain-can-change-the-future-of-iot/. [Accessed 2018].
[66] M. Chiang and T. Zhang, “Fog and iot: An overview of research opportunities,” IEEE Internet of Things Journal, vol. 3, pp. 854–864, Dec 2016.
[67] D. Warren and C. Dewar, “Understanding 5g: Perspectives on future technological advancements in mobile,” GSMA Intelligence, Dec 2014.
[68] R. Munoz, J. Mangues-Bafalluy, R. Vilalta, C. Verikoukis, J. Alonso-Zarate, N. Bartzoudis, A. Georgiadis, M. Payaro, A. Perez-Neira, R. Casellas, R. Martinez, J. Nunez-Martinez, M. R. Esteso, D. Pubill, O. Font-Bach, P. Henarejos, J. Serra, and F. Vazquez-Gallego, “The cttc 5g end-to-end experimental platform: Integrating heterogeneous wireless/optical networks, distributed cloud, and iot devices,” IEEE Vehicular Technology Magazine, vol. 11, pp. 50–63, Mar 2016.
[69] R. Fantacci, T. Pecorella, R. Viti, and C. Carlini, “A network architecture solution for efficient iot wsn backhauling: challenges and opportunities,” IEEE Wireless Communications, vol. 21, pp. 113–119, Aug 2014.
[70] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, “Safeguarding 5g wireless communication networks using physical layer security,” IEEE Communications Magazine, vol. 53, pp. 20–27, April 2015.
[71] L. Xu, J. Xie, X. Xu, and S. Wang, “Enterprise lte and wifi interworking system and a proposed network selection solution,” in 2016 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), pp. 137–138, March 2016.
[72] Y. Zheng, Z. Peng, and V. A. V., “A security and trust framework for virtualized networks and software defined networking,” Security and Communication Networks, vol. 9, no. 16, pp. 3059–3069.
[73] X. Duan and X. Wang, “Authentication handover and privacy protection in 5g hetnets using software defined networking,” IEEE Communications Magazine, vol. 53, pp. 28–35, April 2015.
[74] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, “Device-to-device communication in 5g cellular networks: challenges, solutions, and future directions,” IEEE Communications Magazine, vol. 52, pp. 86–92, May 2014.
[75] H. Shariatmadari, R. Ratasuk, S. Iraji, A. Laya, T. Taleb, R. Jntti, and A. Ghosh, “Machine-type communications: current status and future perspectives toward 5g systems,” IEEE Communications Magazine, vol. 53, pp. 10–17, September 2015.
[76] "Fog Computing and the Internet of Things: Extend," Cisco, [Online]. Available: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf, pp. 5. [Accessed 2018].
[77] M. Rouse, "Edge computing," August 2016. [Online]. Available: http://searchdatacenter.techtarget.com/definition/edge-computing. [Accessed 2018].
[78] CEN-CENELEC-ETSI Smart Grid Coordination Group, “SGCG/M490/G Smart Grid Set of Standards Version 3.1”, Oct-2014, Available Online :

ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Standards_Report.pdf

[79] A. Leonardi, K. Mathioudakis, A. Wiesmaier and F. Zeiger, "Towards the Smart Grid: Substation Automation Architecture and Technologies", Advances in Electrical Engineering, vol. 2014, pp. 1-13, 2014.

[80] Pierre Rust, "Applications for the Internet of Things", Available Online : http://ci.emse.fr/iot/2017/IotApplications.pdf

[81] Hamed Rahimi, Ali Zibaeenejad and Ali Akbar Safavi, "A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies", GlobeCom-IoT, Available Online : https://arxiv.org/ftp/arxiv/papers/1807/1807.03065.pdf

[82] A. Srilakshmi, Jeyasheela Rakkini, K. R. Sekar and R. Manikandan, "A Comparative Study on Internet of Things (IoT) and its Applications in Smart Agriculture", Pharmacognosy Journal, Vol 10, Issue 2, Mar-Apr, 2018, Available Online : http://www.phcogj.com/sites/default/files/PharmacognJ-10_2_260.pdf

[83] R. Williams, E. McMahon,S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach", 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017 doi:10.1109/isi.2017.8004904

[84] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug. 2018. doi: 10.1109/JIOT.2017.2767291

[85] U. Fiore, A. Castiglione, A. De Santis and F. Palmieri, "Exploiting Battery-Drain Vulnerabilities in Mobile Smart Devices," in IEEE Transactions on Sustainable Computing, vol. 2, no. 2, pp. 90-99, 1 April-June 2017. doi: 10.1109/TSUSC.2017.2690148

[86] Xiao, Qinghan & Gibbons, Thomas & , Lebrun. (2009). RFID Technology, Security Vulnerabilities, and Countermeasures. 10.5772/6668. Available Online : https://www.researchgate.net/publication/221787702_RFID_Technology_Security_Vulnerabilities_and_Countermeasures

[87] A. Khalajmehrabadi, N. Gatsis, D. Akopian and A. Taha, "Real-Time Rejection and Mitigation of Time Synchronization Attacks on the Global Positioning System", IEEE Transactions on Industrial Electronics, vol. 65, no. 8, pp. 6425-6435, 2018.

[88] H. Ning, H. Liu and L. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 3, pp. 657-667, 2015.

[89] P. Hao, X. Wang and W. Shen, "A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication," in IEEE Access, vol. 6, pp. 42279-42293, 2018. doi: 10.1109/ACCESS.2018.2859781

[90] M. Shahzad and M. P. Singh, "Continuous Authentication and Authorization for the Internet of Things," in IEEE Internet Computing, vol. 21, no. 2, pp. 86-90, Mar.-Apr. 2017. doi: 10.1109/MIC.2017.33

[91] M. N. Aman, K. C. Chua and B. Sikdar, "Mutual Authentication in IoT Systems Using Physical Unclonable Functions," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1327-1340, Oct. 2017. doi: 10.1109/JIOT.2017.2703088

[92] J. Chauhan, S. Seneviratne, Y. Hu, A. Misra, A. Seneviratne and Y. Lee, "Breathing-Based Authentication on Resource-Constrained IoT Devices using Recurrent Neural Networks," in Computer, vol. 51, no. 5, pp. 60-67, May 2018. doi: 10.1109/MC.2018.2381119

[93] J. Ni, X. Lin and X. S. Shen, "Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 3, pp. 644-657, March 2018.

[94] R. Ravindran, A. Chakraborti, S. Amin, A. Azgin and G. Wang, "5G-ICN: Delivering ICN Services over 5G Using Network Slicing", IEEE Communications Magazine, vol. 55, no. 5, pp. 101-107, 2017.

[95] R. Harel, S. Babbage, “5G Security Recommendations Package #2: Network Slicing”, published by NGMN Alliance, Ver. 01, April 2016. Available Online : https://www.ngmn.org/fileadmin/user_upload/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf

[96] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini and H. Flinck, "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2429-2453, thirdquarter 2018. doi: 10.1109/COMST.2018.2815638

[97] E. Dotaro, “5G Network Slicing and Security”, IEEE SDN newsletter, January 2018, Available Online: https://sdn.ieee.org/newsletter/january-2018/5g-network-slicing-and-security

[98] X. Yao, Z. Chen and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things", Future Generation Computer Systems, vol. 49, pp. 104-112, 2015. Available: 10.1016/j.future.2014.10.010.