Internet of Things: Security Vulnerabilities and Challenges

Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi
Department of Computer Science and Engineering
Frederick University
Cyprus
com.ai@frederick.ac.cy, ch.chrysostomou@frederick.ac.cy, com.hg@frederick.ac.cy

***Abstract*—Internet of Things (IoT) has been given a lot of emphasis since the 90s when it was first proposed as an idea of interconnecting different electronic devices through a variety of technologies. However, during the past decade IoT has rapidly been developed without appropriate consideration of the profound security goals and challenges involved. This study explores the security aims and goals of IoT and then provides a new classification of different types of attacks and countermeasures on security and privacy. It then discusses future security directions and challenges that need to be addressed to improve security concerns over such networks and aid in the wider adoption of IoT by masses.**

Keywords—Internet of Things, attacks, countermeasures, security challenges.

I. INTRODUCTION

Internet of Things allows electronic devices in our surrounding environment to be active participants by sharing information with other members of the network making it possible to recognise events and changes in their surroundings and to act and react autonomously mainly without any human interaction [1]. The advantages of IoT are almost limitless and its applications are changing the way we work and live by saving time and resources, and opening new opportunities for growth, innovation, and the exchange of knowledge between entities. It is predicted that by 2020 Internet of Things will greatly expand with more than 50 billion uniquely identifiable devices (excluding PCs, tablets and smartphones), which is an impressively large number [2]. However, the existence of such a large network of interconnected entities will definitely pose new security, privacy, and trust threats that put all those devices at a high risk, thus harming the affiliated users.

Internet is the foundation and core supporting IoT hence almost all the security threats that lie within Internet propagate to IoT as well. Furthermore, the fast development and wider adoption of IoT devices in our lives signifies the urgency of addressing these security threats before deployment. Although a lot of companies state that their technologies are secured and protected, they are still prone to various types of attacks. Since the interconnected devices have a direct impact on the lives of users, there is a need for a well-defined security threat classification and a proper security infrastructure with new systems and protocols that can mitigate the security challenges regarding privacy, data integrity, and availability in IoT [3].

This paper, after defining the security goals for IoT, it provides a new classification of the most important well known attacks on IoT systems. It introduces the idea of categorising the attacks under four distinct types (i.e., physical, network, software and encryption attacks), to cover the diversity of challenges and threats for all layers in IoT. Furthermore, it suggests a set of guidelines for future security directions for mitigating IoT challenges.

The paper is organised as follows. Chapter II provides an overview of IoT architecture and components. Chapter III explores the IoT security goals. In Chapter IV the literature review of the work done on security of IoT is given. Chapter V provides a classification of the security challenges in IoT Systems. Then Chapter VI establishes new security directions to countermeasure these threats and finally Chapter VII concludes the paper.

II. IOT OVERVIEW

The term Internet of Things was first introduced as an idea in 1999 by Kevin Ashton [4], which has now evolved into a reality that interconnects real world sensors, electronic devices and systems to the Internet:

- Consumer services, smart houses, and smart objects
- Smart energy; smart meters and grids
- Smartphones and Tablets
- Internet connected cars
- Wearable devices; health and fitness monitoring devices, watches, smart clothing, pets smart collars or implanted RFIDs, and even human implanted devices (pacemakers)
- Wireless sensor networks; weather measuring, health care monitoring, industrial monitoring, data loggings, environmental monitoring (water quality, earth sensing fire detection, air pollution monitoring) etc.

A. IoT main enabling technologies

IoT is implemented using a variety of existing network technologies, and more specifically using the following three:

1) Radio Frequency Identification (RFID)

RFID technology using radio frequencies enables the design of microchips for transmitting data in wireless data communication. They use tags (labels) attached on objects for automatic identification acting as electronic barcodes. Tags can either be passive or active. Passive RFID tags are not

978-1-4673-7194-0/15/$31.00 ©2015 IEEE

battery powered and they use the power of the reader's interrogation signal to communicate the ID to the RFID reader. On the other hand, active RFID tags have their own battery supply and can instantiate the communication.

2) Wireless Sensor Networks (WSN)

Wireless Sensor Networks consist of geographically distributed autonomous, low cost, low power small devices that use sensors to monitor physical environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes.

3) Cloud Computing

Cloud computing can enable ubiquitous sensing services and powerful processing of sensing data to be stored and used intelligently for smart monitoring and actuation with the smart devices.

B. IoT Structure

IoT is typically structured into 3 basic Layers, [8]; the Application, the Network Layer, and the Physical Layer, as shown in Fig. 1.

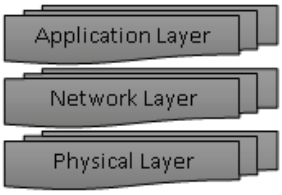

Fig. 1. Internet of Things Architecture

1) Physical Layer

The bottom layer of the architecture is basically the layer responsible for the interconnected devices and its main purpose is to perform device identification and provide service discovery. These devices can be of various types (Arduino, Raspberry, ZigBee, etc.), but in order to be considered as IoT devices they need to utilise communication technology that allow them to connect to one another either directly or indirectly using the Internet; e.g., Arduino with Ethernet connection, a Raspberry Pi with a Wi-Fi connection, a Bluetooth connection, and a low power radio connection [9]. In addition to this, each device needs to have a unique tag that allows it to connect successfully to the network. Ideally, Universally Unique identifiers (UUID) [10] should be used for different objects throughout the Internet that should be burnt onto the device (preferably unchangeable IDs provided by the core hardware); they are typically part of the System-on-Chip or provided by a secondary chip [11]. Currently a device can be coupled with a data sensor device like an RFID or any other sensor network device [12] with a unique ID for the main purpose of identifying it as a unique object.

2) Network Layer

Just like any other Network Layer model this one includes network interfaces, communication channels, network management, information maintenance, and intelligent processing, and is mainly responsible for the communication and connectivity of all the devices in IoT system through the help of multiple communication protocols [13]. There is not any standard protocol for IoT, but the most common protocols that are currently being used are MQTT 3.1 [14] and the Constrained Application Protocol (CoAP) [15]. It is within this layer that the gathered information from the Physical Layer are transmitted to any specific information processing system within the network using Wireless Sensors [16] or to an outside network through existing communication infrastructures like the Internet or a Mobile Network. Each physical device in an IoT system usually sends its information with the use of wireless sensors. These sensors are small, with limited processing and computing power for lower electricity consumption. The data received from the sensors are processed, transmitted wirelessly, and presented to the end user (e.g., human or device). So the network layer aggregates and combines communications from different devices and provides the ability to route communications to any specific device usually via a gateway [17].

3) Application Layer

This layer is service-oriented [18], which ensures the same type of service among the connected devices. It can store data into a database providing storage capabilities to the collected data. Also, just like its name suggests, it facilitates ways for these devices to communicate outside of the device-oriented system with the use of different kind of applications depending on the needs of the users [19]; e.g., Smart Home, eHealth, Smart Transportation, Smart Objects etc.

C. IoT Protocols

Although the architecture of an IoT system is similar to that of the TCP/IP Stack, it does not use the same protocols at the different layers because of the low power devices that are present in the IoT and their required operation of months or years without getting any power recharge. Therefore, less power equals to less computation power available to the devices; hence standard TCP/IP protocols become less ideal and suboptimal for the IoT characteristics and challenges. This raises security concerns as the interoperable IoT protocols and open IoT standards lack the security foundation compared to the TCP/IP Stack protocols.

III. SECURITY GOALS

Because IoT is a relatively new concept, there is a need to define its security goals. To successfully achieve this we need to understand that IoT is an implementation of network technologies and an integration of existing network infrastructures (e.g. wireless sensor networks, RFIDs based sensor networks, Cloud Computing, the Internet etc.). Therefore, all of the security challenges and threats of each network technology are passed by default onto the IoT system that utilises these technologies. Further, there is the possibility of additional security threats that arise from the coexistence and collaboration of the different technologies and the open standards and protocols created for the IoT. The most desirable security objective of IoT is to protect the collected data, since the data collected from physical devices may also include sensitive user information. For this reason the security of any IoT system needs to be resilient to data-related attacks and provide trust and data security and privacy.

A. *Security and Privacy in IoT Definition*

In this paper data security and privacy refers to the protection of any collected or stored data in any IoT system. This means that at any moment the IoT system needs to provide data confidentiality, integrity, and availability. This can be achieved by utilizing authentication, access control, data encryption, and data availability and redundancy through back-ups and etc.

B. *Trust*

Trust is a complicated concept consisting of differ properties and aims. In this paper trust refers to the enforcement of the security goals explained above consisting of the following objectives:

1) Trust relations between each IoT Layer

Proper communication and transition between the different layers of an IoT system and between the different existing nodes is needed to ensure security and privacy of data.

2) Trust for the security and privacy at each IoT layer

Security and privacy goals at each layer in IoT system needs to be preserved under any circumstances providing reliability, integrity, and confidentiality of data.

3) Trust between the user and the IoT system

At a certain point the IoT system will disclose some of the data to the end user and vice versa. Hence, there is a need to provide a level of trust between the IoT system and the end user for the successful employment of the IoT concept. In addition, the user will interact with the IoT system and his actions may impact the correctness of the operation of the system. Thus, there is a need to grade the actions of the user.

The above trust objectives are typically addressed by deploying a Trust Management system, which will ensure the proper functionality of the IoT system regarding privacy, integrity, and availability. Providing an in-depth analysis of Trust Management Systems for IoT is beyond the scope of this paper.

IV. LITERATURE REVIEW

Although security challenges and security mechanisms have been widely studied in various fields (e.g., WSNs), current IoT research has not comprehensively investigated how to provide a proper classification of security challenges. Work in [1], [5], [8] focus on the security challenges of an IoT system; however, most of these papers address only specific types of threats based on specific security objectives. Furthermore, the authors in [22] address the security threats and attacks on RFID systems, which comprise only a subset of the technologies used in IoTs systems. The authors in [29] explore the security challenges of linking IoT to cloud computing. Research in [31] focuses on Jamming attacks that are specific to Wireless Sensor Network. Finally, the authors in [36] provide a survey on privacy and security challenges of IoT. Compared to previous work, our paper aims to provide a more extensive list of security goals, which covers all of the layers and technologies of IoT, and addresses most of the important challenges and threats. Furthermore, a few studies [13], [20], [24], [25] tried to provide proper well-defined security architecture for the IoT based on their security challenges and goals. Although there has been work on the security of RFID systems and Wireless Sensor Networks [23], [26], [32], [42], there is still a need for IoT specific security challenges and goals, as IoT is a combination of existing network technologies. Finally, a number of papers [47], [48], [49], [50], [51], [52] have focused on the issue of trust in IoT on different dimensions. The authors in [53] presented a detailed survey on Trust Management regarding IoT and expanded future directions regarding trust in IoT.

V. CLASSIFICATION OF IOT SECURITY ATTACKS

This paper attempts to capture a broader spectrum of the security vulnerabilities and attacks in IoT systems. Our classification is unique compared to other classifications as it divides the different attacks under four distinct classes; Physical, Network, Software and Encryption attacks. An IoT system can be attacked physically, or attacked from within its network, or from applications on the system, and lastly from attacks on encryption schemes. IoT is implemented using various existing network technologies (Wireless Sensor Networks, RFIDs, Internet, etc.). Thus, there is a need for a proper categorisation of the attacks such that it encapsulates all of the different types of threats, so that better counter measurements can be developed and implemented for securing it. However, it is worth mentioning that Environmental Attacks (Earthquakes etc.) are omitted from this paper as their scope is beyond our research that focuses on intentional attacks from an adversary. A summary of the classification of the attacks is shown in Table 1 below.

TABLE I. CLASSIFICATION OF IOT ATTACKS

<table>
<tr><th>Physical Attacks</th><th>Network Attacks</th><th>Software Attacks</th><th>Encryption Attacks</th></tr>
<tr><td>Node Tampering</td><td>Traffic Analysis Attacks</td><td rowspan="2">Virus and Worms</td><td>Side Chanel Attacks</td></tr>
<tr><td>RF Interference</td><td>RFID Spoofing</td><td rowspan="4">Cryptanalysis Attacks:
a) Ciphertext Only Attack
b) Known Plaintext Attack
c) Chosen Plaintext or Ciphertext Attack</td></tr>
<tr><td>Node Jamming</td><td>RFID Cloning</td><td rowspan="2">Spyware and Adware</td></tr>
<tr><td>Malicious Node Injection</td><td>RFID Unauthorised Access</td></tr>
<tr><td>Physical Damage</td><td>Sinkhole Attack</td><td rowspan="3">Trojan Horse</td></tr>
<tr><td>Social Engineering</td><td>Man In the Middle Attack</td></tr>
<tr><td rowspan="3">Sleep Deprivation Attack</td><td rowspan="2">Denial of Service</td></tr>
<tr><td rowspan="3">Malicious scripts</td><td rowspan="4">Man In the Middle Attack</td></tr>
<tr><td rowspan="2">Routing Information Attacks</td></tr>
<tr><td rowspan="2">Malicious Code Injection on the Node</td><td rowspan="2">Denial of Service</td></tr>
<tr><td>Sybil Attack</td></tr>
</table>

A. Physical Attacks

These kinds of attacks are focused on the hardware components of the IoT system and the attacker needs to be physically close or into the IoT system for the attacks to work. What is more, attacks that harm the lifetime or functionality of the hardware are also included in this category. We will next explore these attacks.

1) Node Tampering

The attacker can cause damage to a sensor node, by physically replacing the entire node or part of its hardware or even electronically interrogating the nodes to gain access and alter sensitive information, such as shared cryptographic keys (if any) or routing tables, or impact the operation of higher communication layers [26].

2) RF Interference on RFIDs

A Denial of Service attack can be implemented on any RFID tag by creating and sending noise signals over the Radio Frequency signals which are used by the RFIDs for communication [25]. The noise signals will interfere with the RFID signals hindering communication.

3) Node Jamming in WSNs

This is similar to the Radio Frequency Interference physical attack explained earlier for the RFIDs with the difference that this attack is based on the WSNs. The attacker can interfere with the radio frequencies of the wireless sensor nodes, jamming the signals and denying communication to the nodes. If the attacker manages to jam key sensor nodes he can successfully deny service of the IoT [31].

4) Malicious Node Injection

The adversary can physically deploy a new malicious node between two or more nodes of the IoT system, hence controlling all data flow from and to the nodes and their operation; this is also known as Man in The Middle Attack.

5) Physical Damage

The adversary can physically damage devices of the IoT network for his own gain. This kind of attack is an attack that deals with security of the area or building that hosts the IoT system. It differs from Node Tampering attack as in this situation the adversary tries to directly damage the IoT system with the purpose of impacting the availability of service.

6) Social Engineering

The attacker manipulates users of an IoT system, to extract private information or to perform certain actions that would serve his goals. This kind of attack is put under the physical attacks category because the attacker needs to physically interact with the IoT network users to achieve his goals.

7) Sleep Deprivation Attack

Most sensor nodes in the IoT system are powered by replaceable batteries and are programmed to follow sleep routines to extend their battery life. This attack, keeps the nodes awake which will result in a more power consumption, and will cause the nodes to shut down.

8) Malicious Code Injection

The attacker compromises a node by physically injecting it with malicious code that would give him access to the IoT system; e.g. imagine an attacker inserting a USB stick with harmful software (i.e. virus) onto the node. This would mean that the attacker could gain full control of the node or even control of the whole system.

B. Network Attacks

These attacks are centred on the IoT system network and the attacker does not necessarily need to be close to the network for the attack to work.

1) Traffic Analysis Attacks

An attacker can sniff out the confidential information or any other data flowing from the RFID technologies because of their wireless characteristics [21]. Also, in almost all of the attacks an attacker first tries to gain some network information before he employs his attack. This is done using sniffing applications like port scanning application, packet sniffer applications etc. [34].

2) RFID Spoofing

An attacker spoofs an RFID signals to read and record a data transmission from an RFID tag. Then the attacker can send his own data containing the original tag ID, making it appear to be valid, hence the attacker gains full access to the system pretending to be the original source [22].

3) RFID Cloning

An attacker clones an RFID tag by copying data from the victims RFID tag, onto another RFID tag. Although the two RFID tags have identical data, this method does not replicate the original ID of the RFID, making it possible to distinguish between the original and the compromised, unlike the event in the RFID spoofing attack.

4) RFID Unauthorised Access

Because of the lack of proper authentication mechanisms in the majority of RFID systems, tags can be accessed by anyone. This automatically means that the attacker can read, modify or even delete data on the RFID nodes [24].

5) Sinkhole Attack

The attacker lures all traffic from WSN nodes, hence creating a metaphorical sinkhole. This type of attack breaches the confidentiality of the data and also denies service to the network by dropping all the packets instead of forwarding them to the desired destination [27].

6) Man In the Middle Attack

The attacker over the network manages to interfere between two sensor nodes, accessing restricted data, violating the privacy of the two nodes by monitoring, eavesdropping and controlling the communication between the two sensor nodes [29]. Unlike the Malicious Node Injection from the Physical Attacks category, the attacker does not necessarily need to be physically there for this kind of attack to be successful, but relies solely on the network communication protocols of an IoT system.

7) Denial of Service

An attacker can bombard an IoT network with more traffic data that it can handle which can result in a successful Denial of Service attack.

8) Routing Information Attacks

These are direct attacks that the adversary by spoofing, altering or replaying routing information can complicate the network and create routing loops, allowing or dropping traffic, sending false error messages, shortening or extending source routes or even partitioning the network [28]; e.g. Hello Attack [32] and Blackhole Attack.

9) Sybil Attack

A malicious node (i.e. Sybil Node), is a single node that claims the identities of a larger number of nodes, and impersonating them. This kind of attack leads to false information being accepted by the neighbouring WSN nodes; e.g. imagine a WSN voting system where one Sybil node votes more than once [30], or a Sybil node being selected as part of a routing path.

C. Software Attacks

Software attacks are the main source of security vulnerabilities in any computerised system. Software attacks exploits the system by using Trojan horse programs, worms, viruses, spyware and malicious scripts that can steal information, tamper with data, deny service and even harm the devices of an IoT System.

1) Phishing Attacks

The attacker gains access to confidential data by spoofing the authentication credentials of a user, usually through infected emails or phishing web sites [33].

2) Virus, Worms, Trojan Horse, Spyware and Aware

An adversary can infect the system with malicious software resulting in a variety of outcomes; stealing information, tampering data or even denial of service [35].

3) Malicious Scripts

Usually the IoT network is connected to the Internet. The user that controls the gateway can be fooled into running executable active-x scripts which could result in a complete system shut down or data theft [35].

4) Denial of Service

An attacker can execute DoS or distributed denial of service DDoS attacks on the affected IoT network through the application layer, affecting all users in the network. This kind of attack can also block the legitimate users from the application layer giving full application layer access to the attacker; databases and private sensitive data [36].

D. Encryption Attacks

These attacks are solely based on breaking the encryption scheme being used in an IoT system.

1) Side channel Attacks

Using particular techniques (i.e. Timing, Power, Fault and Electromagnetic Analysis) on the encryption devices of an IoT system, the attacker can retrieve the encryption key being used for encrypting and decrypting data.

2) Cryptanalysis Attacks

These attacks assume the possession of ciphertext or plaintext and their purpose is to find the encryption key being used by breaking the encryption scheme of the system. Examples of cryptanalysis attacks on IoT systems include Known-plaintext attack, Chosen-plaintext attack, Chosen Ciphertext attack, and Ciphertext-only attack.

3) Man In the Middle Attack

When two users of an IoT system A and B, exchange keys during a challenge-response scenario, so as to establish a secure communication channel, an adversary positions himself between them on the communication line. The adversary then intercepts the signals that A and B send to each other and attempt to interfere by performing a key exchange with A and B separately. The adversary will then be able to decrypt/encrypt any data coming from A and B with the keys that he shares with both of them. Both A and B will think that they are talking with each other.

VI. Security Future Directions

In this Section we will provide future directions for security based on the challenge classification presented earlier. An IoT system consists of three different layers each with vulnerabilities and security attacks. To address these attacks and to successfully protect the IoT system, this section presents a multi-layered security approach that should be structured to give an optimal layered protection at each layer in an IoT system as shown on the next page in Table II. A detailed description of the table is explained below.

A. IoT Physical Layer Security

a) Secure Booting: Authentication and the integrity of the software on the device should be verified using cryptographic hash algorithms, which would provide digital signatures. However, because of the low processing power on most of the devices and their need for ultra-low power consumption most cryptographic hash algorithms cannot be implemented, apart from NH and WH cryptographic hash functions that are optimal for ultra-low power consumption devices [37], [38].

b) Device authentication: When a new device is introduced to the network, it should authenticate itself before receiving or transmitting data, to ensure it is identified correctly before authorisation and keeping malicious devices out of the system.

c) Data integrity: Error detection mechanisms should be provided at each device, to ensure no tampering of sensitive data occurs. Low power consumption mechanisms like Cyclic Redundancy Checks (CRC), Checksum, Parity Bit are preferred, but for more secure error detection method WH cryptographic hash function should be applied [39].

d) Data Confidentiality: All RFID Tags, IDs and data should be encrypted on each device before transmission of data to ensure confidentiality. However, because of the ultra-low power consumption, strong cryptographic encryption functions like AES cannot be implemented. Instead Blowfish or RSA have lower power consumption and less processing power and can be successfully implemented on the physical layer devices.

e) Anonymity: In some cases hiding sensitive information like the location and identity of nodes is crucial. Although Zero-Knowledge [40] approach would be the optimal solution for anonymity, it cannot be implemented on low power devices as it is a very strong algorithm and needs a lot of processing power, hence K- anonymity [41] approach best fits the job for low power devices such as the devices used in an IoT system.

B. IoT Network Layer Security

a) Data privacy: Illegal access to the sensor nodes can be prevented, using authentication mechanisms and point to point encryption [42].

b) Routing security: Secure routing is vital to the acceptance and use of sensor networks for many applications, but the majority of used routing protocols are insecure [43]. However, security of routing can be ensured by providing multiple paths for the data routing which improves the ability of the system to detect an error and keep performing upon any known of failure in the system [44]. Also, encryption and authentication mechanisms increase the security level of routing data.

c) Data integrity: Using cryptographic hash functions, the integrity of the data received on the other end is confirmed. In case of prove of tampering of data, error correction mechanisms could be introduced to mitigate the problem.

C. IoT Application Layer Security

a) Data security: Authentication Encryption and Integrity mechanisms are critical at this level for insuring the privacy of the whole system and protecting against data theft; it prevents unauthorised access to the system and ensures the confidentiality of the system data.

b) Access Control Lists (ACLs): Setting up policies and permissions of who can access and control the IoT system, is a crucial part as this ensures the privacy of the data, and the well being of the system. ACLs can block or allow incoming or outgoing traffic, and give or block access to requests from different users inside or outside of the network.

c) Firewalls: This is an extra effective layer of security that will help block attacks that authentication, encryption and ACLs would failed to do so. Authentication and encryption passwords can be broken if weak passwords were selected. A firewall can filter packets as they are received, blocking unwanted packets, unfriendly login attempts, and DoS attacks before even authentication process begins.

d) Anti-virus, Anti-spyware and Anti-adware: Security software like antivirus or anti spyware is important for the reliability, security, integrity and confidentiality of the IoT system.

TABLE II. SECURITY COUNTERMEASURES

IoT Layer	Counter Attacks for the Specific Layers	Counter Attacks for All Layers
Physical Layer	1) Secure Booting for all IoT devices a) Low power Cryptographic Hash Functions 2) Device Authentication using Low Power Techniques a) Data Integrity b) CRC – Cyclic Reduntancy Check c) Checsum d) Parity Bit e) WH Cryptographic Hash Function 3) Data Confidentiality a) Encryption Algorithms like Blowfish and RSA 4) Data Anonimity a) K- Anonimity	1) Risk Assessment b) Finding New Threats c) Applying Updates d) Applying Patches e) Providing Improvements f) Upgrading Systems 2) Intrusion Detection Mechanisms specific to IoT Systems 3) Securing the IoT Premises a) Physical Barriers b) Intrusion Detection Alarms c) Monitoring Devices d) Access Control Devices e) Security Personel 4) Trust Management a) Trust relation between layers b) Trust of Security and Privacy at each layer c) Trust betweeen IoT and User
Network Layer	1) Secure Communication between the devices a) Network Authentication – challenge-response mechanisms b) Point-to-Point Encryption for the confidentiality of the transmited Data c) Cryptographic Hash Functions for the Inegrity of the transmited Data 2) Implementation of Routing Security a) Use of Multiple Paths b) Encrypting Routing Tables c) Hashing Routing Tables 3) Secure User Data on the Devices a) Data Authentication b) Data Confidentiality; Encryption Schemes of encrypting the data c) Data Integrity; Cryptographic hash functions	
Application Layer	1) Data Security a) Authentication; biometrics, passwords, etc. b) Confidentiality; Strong Encryption Schemes (AES) c) Integrity; Cyrptographic Hash Functions 2) Access Control Lists (ACLs) 3) Firewalls 4) Protective Software a) Anti-virus b) Anti-adware	

To insure the continued protection of an IoT system and maintain its trustworthiness, Risk Assessment, Intrusion Detection, Physical Security and Trust Management should be mandatory at all layers in IoT.

a) Risk Assessment is fundamental for the continuing security of the system, by discovering new threats, applying updates and patches to the firmware on the system devices, as well as providing improvements in the existing security structure [45].

b) Intrusion Detection mechanisms at all three layers, is very important as it would alarm the user in the occurrence of any suspicious activity at any of the three layers [46].

c) Securing the premises is perhaps the most important security feature that IoT needs, as it physically secures the IoT devices; i.e. sensor nodes, computers, firewalls, data servers etc. The security of the IoT devices is achieved by using Physical Barriers to block any unauthorised people, Intrusion Detection Systems to monitor any strange behaviour, Access Control to make sure only legible users enters the premises of the IoT and even Security personnel to ensure total security of the IoT devices.

d) A Trust Management System needs to be launched for the trustworthiness of the whole IoT System throughout its execution. The trust management entity will ensure that the security goals explored in this paper are enforced and that the security mechanisms are deployed successfully.

Furthermore, security of almost all cryptographic systems depends on the randomness of the secret key, but because they consume too much power it is hard to be implemented on IoT devices. Similar to this, Trust Management systems require a lot of power consumption and processing power to dynamically account for changes in behaviour or reputation of the entities involved. Research should be done in creating new secure encryption and authentication mechanisms for ultra-low power devices, as well as new strong low-power-use trust management systems. In addition to that, standard policies, regulations, and frameworks should be devised to ensure stability, security, and reliability. Finally, new security protocols should be developed depending on the scheme being used in an IoT system; e.g., eHealth etc.

VII. Conclusion

IoT has been a major research topic for almost a decade now, where physical entities would interconnect using existing network technologies. Due to its rapid progression many threats in security and privacy exists, which hinder its development. This paper explored the security goals required for a secure IoT system, and classified its security challenges and issues using a new unique classification method consisting of four classes of attacks; Physical, Network, Software, and Encryption Attacks. Based on this classification, we then highlighted the security countermeasures needed to successfully secure an IoT system. Furthermore, future directions for security for IoT were discussed. This classification could be used as a framework to categorise attacks, as well as to guide the secure deployment of IoT systems. As future work, we aim to investigate the interaction between heterogeneous IoT devices and its impact on security. Further, we aim to investigate weaknesses in trust management systems proposed for IoT systems.

References

[1] D. Singh, G. Tripathi, and A.J. Jara. "A survey of Internet-of-things: Future vision, architecture, challenges and services." In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pp. 287-292. IEEE, 2014.

[2] J. Bradley, J. Barbier, and D. Handler. "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience CISCO Whitepaper." White Paper, Cisco Systems Inc (2013).

[3] M. Friedemann, and C. Floerkemeier. "From the Internet of Computers to the Internet of Things." In From active data management to event-based systems and more, pp. 242-259. Springer Berlin Heidelberg, 2010.

[4] K. Ashton, "That 'internet of things' thing." RFiD Journal 22, no. 7 (2009): 97-114.

[5] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, pp. 648-651. IEEE, 2012.

[6] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of things." In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 5, pp. V5-484. IEEE, 2010.

[7] D. Xu, L. Yang, and L. Jiang, "Research and Design of IOT Gateway." In 2015 International Industrial Informatics and Computer Engineering Conference. Atlantis Press, 2015.

[8] Y. Song, "Security in Internet of Things." (2013).

[9] P. Fremantle, "A Reference Architecture for the Internet of Things", [Online]. Available: http://wso2.com, White Paper, 2014

[10] P. J. Leach, M. Mealling, and R. Salz, "A universally unique identifier (uuid) urn namespace." (2005).

[11] Z. Song, A. A. Cárdenas, and R. Masuoka, "Semantic middleware for the Internet of Things." In IoT. 2010.

[12] Y. Zhang, "Technology Framework of the Internet of Things and its Application." In Electrical and Control Engineering (ICECE), 2011 International Conference on, pp. 4109-4112. IEEE, 2011.

[13] X Yang, Z Li, Z Geng, and H Zhang, "A Multi-layer Security Model for Internet of Things." In Internet of Things, pp. 388-393. Springer Berlin Heidelberg, 2012.

[14] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks." In Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on, pp. 791-798. IEEE, 2008.

[15] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)." (2014).

[16] J. Yick, B. Mukherjee, and D. Ghosal. "Wireless sensor network survey." Computer networks 52, no. 12 (2008): 2292-2330.

[17] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29, no. 7 (2013): 1645-1660.Asd

[18] R. Khan, S. U. Khan, R. Zaheer, and S. Khan "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges." In FIT, pp. 257-260. 2012.

[19] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29, no. 7 (2013): 1645-1660.

[20] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)." Perception 111, no. 7 (2015).

[21] B. Khoo, "RFID as an enabler of the internet of things: issues of security and privacy." In Internet of Things (iThings/CPSCom), 2011

International Conference on and 4th International Conference on Cyber, Physical and Social Computing, pp. 709-712. IEEE, 2011.

[22] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks." Gen 15693 (2010): 14443.

[23] M. Burmester, and B. De. Medeiros, "RFID security: attacks, countermeasures and challenges." In The 5th RFID Academic Convocation, The RFID Journal Conference. 2007.

[24] R. Uttarkar, and R. Kulkarni, "Internet of Things: Architecture and Security."

[25] L. Li, "Study on security architecture in the Internet of Things." In Measurement, Information and Control (MIC), 2012 International Conference on, vol. 1, pp. 374-377. IEEE, 2012.

[26] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks." Communications of the ACM 47, no. 6 (2004): 53-57.

[27] V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network." International Journal of Application or Innovation in Engineering & Management 2, no. 2 (2013).

[28] D. Wu, and G. Hu, "Research and improve on secure routing protocols in wireless sensor networks." In Circuits and Systems for Communications, 2008. ICCSC 2008. 4th IEEE International Conference on, pp. 853-856. IEEE, 2008.

[29] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS) 1, no. 2 (2011): 136-146.

[30] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses." In Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259-268. ACM, 2004.

[31] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs." Communications Surveys & Tutorials, IEEE 11, no. 4 (2009): 42-56.

[32] M. A. Hamid, M. Mamun-Or-Rashid, and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense." IEEE ICNEWS (2006): 2-4.

[33] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing." Communications of the ACM 50, no. 10 (2007): 94-100.

[34] B. S. Thakur, and S. Chaudhary, "Content sniffing attack detection in client and server side: A survey." International Journal of Advanced Computer Research (IJACR) 3, no. 2 (2013): 10.

[35] H. Tobias, et al. "Security Challenges in the IP-based Internet of Things." Wireless Personal Communications 61, no. 3 (2011): 527-542.

[36] C. M, Medaglia, and A. Serbanati. "An overview of privacy and security issues in the internet of things." In The Internet of Things, pp. 389-395. Springer New York, 2010.

[37] 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 Berlin Heidelberg, 2004.

[38] M. Feldhofer, and C. Rechberger, "A case against currently used hash functions in RFID protocols." In On the move to meaningful internet systems 2006: OTM 2006 workshops, pp. 372-381. Springer Berlin Heidelberg, 2006.

[39] J. P. Kaps, "Cryptography for ultra-low power devices." PhD diss., WORCESTER POLYTECHNIC INSTITUTE, 2006.

[40] U. Feige, F. Amos, and S. Adi,. "Zero-knowledge proofs of identity." Journal of cryptology 1, no. 2 (1988): 77-94.

[41] L. Sweeney, "k-anonymity: A model for protecting privacy." International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10, no. 05 (2002): 557-570.

[42] G. Peretti, V. Lakkundi, M. Zorzi, "BlinkToSCoAP: An End-to-End Security Framework for the Internet of Things." (2015).

[43] X. F. Wang, "Research on Security Issues of the Internet of Things." In Advanced Materials Research, vol. 989, pp. 4261-4264. 2014.

[44] Z. Xu, Y. Yin, and J. Wang, "A density-based energy-efficient clustering algorithm for wireless sensor networks." International Journal of Future Generation Communication and Networking 6, no. 1 (2013): 75-86.

[45] C. Liu, Y. Zhang, J. Zeng, L. Peng, and R, Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology." In Natural Computation (ICNC), 2012 Eighth International Conference on, pp. 874-878. IEEE, 2012.

[46] A. Patcha, and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer Networks 51, no. 12 (2007): 3448-347.

[47] D. Chen, G. Chang, D. Sun, J. Li, J. Jia and X. Wang "TRM-IoT: A trust management model based on fuzzy reputation for internet of things." Computer Science and Information Systems 8, no. 4 (2011): 1207-1228.

[48] F. Bao and I. Chen, "Trust management for the internet of things and its application to service composition", in Proc. of IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012, pp.1-6.

[49] F. Bao, I. Chen and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems", in Proc. of IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), (2013), pp.1-7.

[50] M. Nitti, R. Girau, L. Atzori, A. Iera and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things", in Proc. of IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), (2012) pp. 18-23.

[51] Y. Liu and K. Wang, "Trust control in heterogeneous networks for Internet of Thing", in Proc. of International Conference on Computer Application and System Modeling (ICCASM), (2010), pp.632-636.

[52] D. Gessner, A. Olivereau, A.S. Segura and A. Serbanati, "Trustworthy infrastructure services for a secure and privacy-respecting internet of things", in Proc. of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), (2012) pp.998-1003.

[53] Z. Yan, P. Zhang, A. V. Vasilakos, "A survey on trust management for Internet of Things." Journal of network and computer applications 42 (2014): 120-134.