Internet of Things (IoTs): Architecture, Evolution, Threats and Defense

Ahmed Redha Mahlous[†]

[†]College of Computer and Information Sciences, Prince Sultan University, Riyadh, KSA

Summary
The exponential growth of devices connected to the network has resulted in the development of new Internet of Things (IoT) applications and online services. In recent years, the research in generic Internet of Things (IoT) attracts a lot of practical applications including smart home, smart city, smart grid, industrial Internet, connected healthcare, smart retail, smart supply chain and smart farming. In this paper we surveyed some categories of popular security issues in the IoT and their corresponding proposed solutions. We summarize the recent researches in IoT security field and try to discuss the underemployment topics in this field.

Key words:
IoT, Attacks, Security, Confidentiality, RFID, Botnet

1. Introduction

The development of Information Technology (IT) along with the persistent need to ease communication between people and devices has led to what is called the Internet of Things (IoT). It basically connects various objects that are embedded in the environment to efficiently collect and share data without the need for human intervention [1].
The use of IoTs devices has increased exponentially over the recent time and these devices do more processing of sensitive data. A lot of security concerns have been found and reported in the IoTs world. Recently, many malware are targeting the IoTs and a lot of research reveals that in most cases there are either no security controls or the security controls are not enough on the IoT design and deployment which leave the IoT environment always a good target for malware infection and illegal utilization and mass exploitation as a Cybersecurity weapon "botnet" [2].
While IoT is undoubtedly a blessing to the world of technology, there is a need to address security and privacy issues that mushrooms when implementing the technology in homes, industries, and even cities. It has been noted [3] that IoT leverages actuators; sensors, readers and RFID tags to enable the communication process take place between the physical and digital worlds. The researchers project that by 2020, there will be over 24 billion connected devices while the worth of IoT at that time will be $1.3 trillion for mobile data and network providers. With that in mind, it is unimaginable having such some linked devices that are insecure. Readers in stores use confidential credentials from people's credit card; connected cars deliver real-time location of vehicles while actuators enable industrial components to communicate and automate processes. Tampering with any of the methods that allow interconnectivity can cause anything from stolen personal information to large-scale stall in industrial operations. Because of the expected increase in connected devices in the future, it is likely the cyber attacks and intrusions on these devices, networks and gateways are going to increase. For IoT to have a consistent growth across all sectors, there is need to fortify the security of every IoT component.
For that matter, this paper seeks to survey various literatures that elaborate on security issues relating to IoT. The purpose is to augment these studies and come up with useful recommendations that can assist policymakers and stakeholders in creating ad hoc and long-term strategies to avert security challenges that may drag down the amelioration of IoT. The survey of literature will also note that gaps in the existing studies and recommends areas where future researchers must focus to develop a holistic IoT security approach.
Section 2 presents IoT architecture. Section 3 considers some types of threats and attacks affecting IoTs, while Section 4 lists some IoT security solutions. Section 5 presents some IoT Security analysis, trends and evolution while Section 6 concludes the paper.

2. IoT Architecture

In this section we will review the standard IoT architecture that can be split into three basic layers [4] as shown in Fig. 1, however some industries could have more or lower layers depend on the industry

Manuscript received January 5, 2019
Manuscript revised January 20, 2019

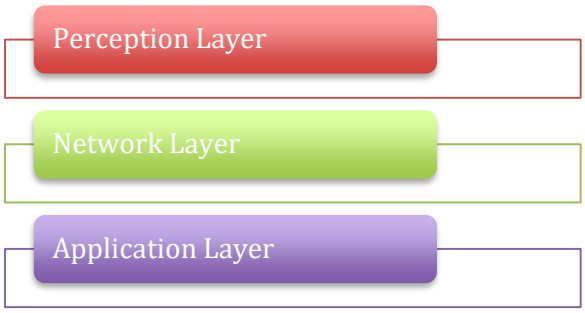

Fig. 1 IoT Architecture

2.1 Perception layer

The first layer is the perception layer, which is, the physical devices such as the sensors and actuators that communicate with each other or with other devices using a standard wireless protocols. The objective of this layer is to collect all the information from the sensors and actuators then, sent it to the network layer.

2.2 Network layer

The second layer called the network layer, which handles the data that travelled between smart devices in the IoT system in addition to the network devices and the servers. Usually, at this layer, a range of technologies are used, such as Routers, Switches and Cloud computing that processes and send the data to the required application layer where the user can read the data.

2.3. Application layer

Application layer is the layer where the user can read the required information that has been transmitted through the network layer after being processed by the perception layer.

3. Types of Threats and Attacks Affecting IoTs

Combating attacks and ensuring that the implementation of IoT in various sectors of the economy implies first identifying forms of vulnerabilities and specific threats that can ravage IoT devices. Protecting interconnected devices from data intrusions such as malware attacks, sniffing, DoS and DDoS, ransomware, identity theft among others can only be successful if users know the techniques the attackers will use to hack into their systems. In the following section we survey different threats and attacks to the IoT devices.

3.1 Trust, Privacy and Security [3]:

The authors follow a cognitive approach to make IoT vision a reality by taking into consideration trust, privacy and security. The context of IoT explained by the authors espouses a fourfold structure (nodes): the people, process, smart object and technology. The authors note that people are responsible for making an IoT system safe and the extent of safety provided depends on their knowledge and skills as well as laws and regulations that govern data sharing and networking. The process node performs tasks and computations by handling requests based on the security and privacy policies in its jurisdiction. The intelligent objects include sensors, actuators, and equipment that are designed to conform to particular security standards. The technological ecosystem comprises of multiple tech-based solutions such as software designs, development of algorithms, privacy protocols and engineering of trust procedures.

3.2 Sybil attack [5]

An example of an attack presented by the authors is the Sybil attack that modifies the node with the aim of falsifying the information passing through the network layer to the application layer. Sinkhole attack is a form of social engineering and an attack on the transport layer that makes a compromised node look legitimate. The affected node tricks the system that it is healthy, and sends fake messages. A continued sinkhole attack can proliferate to a Denial of Service (DoS) attack. Authors also highlighted how sleep deprivation attack pushes sensor nodes using batteries to use more energy by depriving the nodes from their ability to sleep. This causes the sensor nodes to shut down unexpectedly, thus affecting service delivery.

3.3 Physical/Perception layer attack [6]:

Authors highlighted the corresponding attack to the Physical/Perception Layer. They noted that the perception layer is significantly affected by hardware tampering, fake node injection and identity theft. Attackers can alter the node's settings or even orchestrate DoS attacks and then replace the nodes altogether. Attackers can reconfigure the node so they can access the gateway keys, cryptographic keys and other essential authentication keys used by the layer to communicate to the upper layers. The nature of the nodes in this segment does not allow the use of robust protection and security measures, and thus they are vulnerable to many forms of attacks. The availability and integrity of data are profoundly affected in case of attacks in this layer.

3.4 On Building Trust in IoT [7]:

Authors addressed various security and privacy challenges that face IoT devices. They focused their research on approaches that provide flexible management of security pairing of devices. They also proposed an effective method that automatically identifies devices based on their behavior patterns and discover compromised IoT devices.

3.5 A Case Study of a Web Camera [8]:

Authors discussed the threats related to a compromised IoT device and provide a case study of an IP camera. They studied the IP camera and analyze it by inspecting the network services and the communications between the devices. Then they exposed the weaknesses of the camera, which consists mainly of three major weaknesses, the unencrypted traffic between the camera and the server, the brute forcible URL of the video streaming and the plaintext stored credentials. Finally, they suggest some solution to fix the security flaws found in the camera.

3.6 A Taxonomy of IoT: Security and Privacy Threats [9]:

This study aims to propose taxonomy in order to categorize IoT's objects, so security and privacy issues would be fully addressed. The evaluation process shows a slight pattern that emphasizes a relation between Object Characteristics and Security and Privacy concerns in which the higher the degree of the former raises the chance for more vulnerability to the latter as shown in Fig. 2. The authors also stated that more test samples are needed in order to detect a clear pattern, which could help in creating valuable security design principles for future IoT projects.

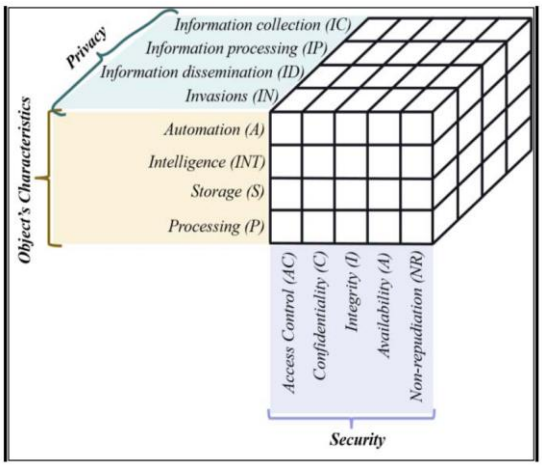

Fig. 2 [9] Three dimensions taxonomy of IoT privacy and security based on objects' characteristics.

3.7 Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models [10]:

This paper investigates security concerns and issues for Industrial Internet of Things (IIoT). The researchers attempted to survey as many IIoT security concerns and issues as possible and provided possible consideration for them. They focused on Cisco and Microsoft Azure reference models and especially data accumulation and abstraction layers, which has never been explored for their security concerns. They discussed possible security challenges in these layers for both Cisco and Azure architecture models and then did a segmentation of threats based on security vulnerabilities and attacks as shown in Fig. 3.

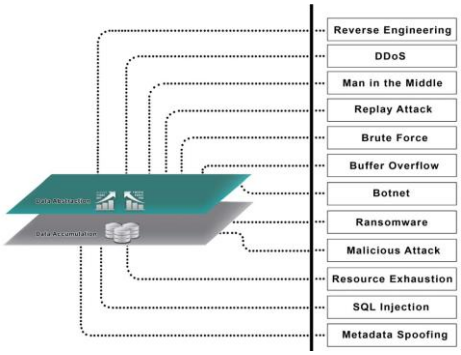

Fig. 3 [10] Summary of security threats within layer 4 and 5

3.8 The Security of Smart Homes: Issues and Solutions [11]:

Many households today contain smart devices for different purposes such as coffee making, smart fridges, smart homes … etc. in this paper the authors talked about the general security issues associated with IoT devices in homes and proposed different solutions to tackle such challenges in order to protect smart home devices. The author's focus was on security and privacy. They come up with a security classification of threats into three different levels: low-level, intermediate-level, and high-level, and different solutions have been proposed for each security threat category.

3.9 IoT Security: Challenges and Solutions for Mining [12]:

The paper highlighted the mass adoption of Internet of Things (IoTs) devices and the new challenges that face the Internet because of those IoIs that have been implemented with minimum to none security practices. Researchers talked about those risks and issues to explain the needed actions to be completed by researchers and government entities in order to standardize and find a solution that is

scalable and flexible. Furthermore, authors went in depth to explain the issue of IoT in mining as Western Australian Mining and Resources Sector (WA) has been one of the early adopters for IoT. Finally authors illustrated the majority of issues that can be managed through a better governance model on IoT standards, IoT security, IoT mining standards, IoT policies and frameworks.

4. IoT security Solutions

While it can be difficult to shield away all the threats because of the behavior and nature of IoT nodes, some practices and security measures can be put in place to bolster the security of IoT and associated components. During the development of IoT devices, security tests should be made at every level to ensure that at the end of the lifecycle, every element and system is highly secured. Indeed, for the growth of IoT, attacks, and threats should not derail this technological development. In this section we highlight some proposed solutions that can be adopted to counter the attacks to the IoT devices.

4.1 Cyber Hygiene' Practices for the Internet of Things (IoT)[13]:

Author in this paper showed that organizations must adapt to the escalating Cybersecurity concerns by coming up with measures that will keep attacks away. The author noted that the best way of handling these security issues is by conducting awareness campaigns, so that the lowest layer node (people) can practice secure habits when handling IoT devices and processes. Furthermore, the authors recommended informing the public about data usage, control and security policies such as the Digital Rights Management (DRM) agreements. Also legislators need to have open discourses with clients in case of breaching such contracts or infringing digital copyrights.

4.2 Framework for Privacy Preservation in IoT through Classification and Access Control Mechanisms [14]:

Authors came up with a framework that classifies data and access control mechanism that fosters privacy when IoT collects and transmits personal identifiable data. The authors noted that a digital certificate must identify every user sending a query, and data in transit must be encrypted.

4.3 Smart Home [15]:

Authors illustrated a software design that can help in averting attacks that may intercept data during communication between sensors and servers. They proposed to use RSA and AES as security algorithms to prevent data interceptions and a QR codes as a method of authorization, which cannot be easily circumvented.

4.4 Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling [16]:

In this paper the authors discussed the complexity of the intrusion detection in the Era of IoT. With the distributed IoT devices and the communication between their different nodes, a security breaches such as Hijacking the sensors and Man-In the Middle have a great impact on the entire IoT Network. The authors addressed this problem by proposing hierarchical structure to reduce the network traffic caused by node-to-node communications, and narrowing the number of packets inspected by IDS to enhance the detection performance. They also proposed to consider traffic filtering and sampling mechanisms as shown in Fig. 4.

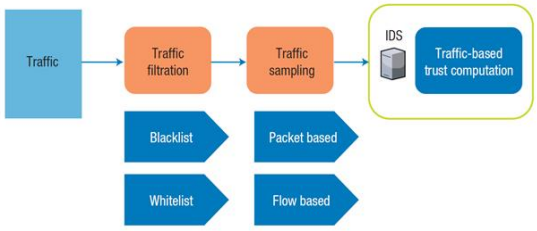

Fig. 4 [16] Traffic filtration and sampling mechanisms

4.5 Deploying Robust Security in Internet of Things [17]:

In this paper, the authors investigated the inevitable risk that is related to security offloading because of recent incidents related to IoT security. They proposed a stochastic model to capture the different security risks of an IoT system and a framework for an efficient deployment of a robust IoT architecture.

4.6 Securing the Internet of Things (IoT):

Security Taxonomy for IoT [18]:

Due to the billions of connected IoTs devices and the huge amount of data that is collected and transmitted by those devices, authors raised the concerns about identity and data theft, device manipulation, data falsification, server/network manipulation, and subsequent impact to application platforms.

4.7 Authentication of IoT Device and IoT Server Using Secure Vaults [19]:

The authors discussed the importance of the authentication between the different IoT System components: IoT device, IoT server and a user interface as shown in Fig. 5.

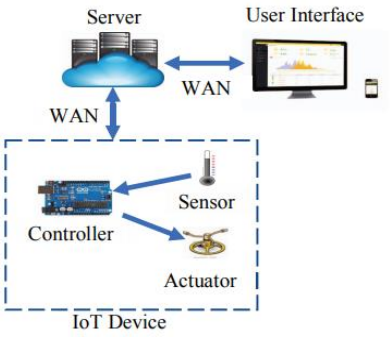

Fig. 5 [19] System Architecture

The IoT device is responsible for collecting the data generated by the sensors connected to it and uploading them to the server. In many cases, it also processes the data before uploading to the server. The IoT device communicates with the IoT server through a wide area network. This IoT system is accessible to the user using a web and/or a mobile interface. Authentication that is based on password is simple and vulnerable to side-channel and dictionary attacks. The author discussed the mutual authentication mechanism (multi key or multi password). The Author called their secret key a secure vault. The algorithm has been tested on one IoT device to prove its efficiency. Table. 1 indicates the growing in the world.

4.8 SDN-Based Data Transfer Security for Internet of Things [20]:

Authors in this paper proposed a protocol based on SDN (Fig. 5) to reduce network latency, and properly manage dataflow to ensure the network run safely. They used middle box in SDN-based IoT to manage dataflow, and improve the stability and security of the network. The experimental results demonstrate that the proposed M-G model and corresponding protocols managed dataflow in middle boxes effectively, and improved the overall IoT network security and stability.

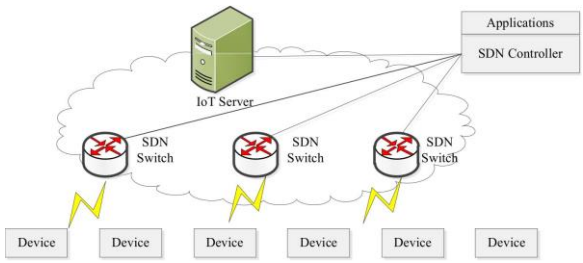

Fig. 6 [20] SDN-based IoT architecture.

4.9 Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks [21]:

The paper emphasizes on the design of a new secure lightweight three-factor remote user authentication scheme for HIoTNs, called the user authenticated key management protocol (UAKMP). The three factors used are the user smart card, password, and personal biometrics. Authors discussed several functionality features and provided detailed descriptions of all phases of UAKMP. They illustrated how UAKMP can successfully prevent some possible well-known attacks such as user impersonating attack. Finally, they showed how UAKMP is more secure as compared to other existing schemes.

4.10 A Software Defined Network-Based Security Assessment Framework for CloudIoT [22]:

In this paper, authors analyzed the dataflow over the CloudIoT, and proposed an SDN-based three-layer indication framework consisting of 23 indicators. To evaluate the importance of these indicators, they published an online survey to invite experts to rate the indicators. Based on the feedback, they presented three different methodologies to generate the aggregate rating to gain the weights.

4.11 Applying Security Patterns for authorization of users in IoT Based Applications [23]:

This study describes patterns for authentication of an unsecured IoT based application, especially in the context of healthcare applications where authorization of the users is a primary concern. Three procedural patterns were discussed including documentations of security goals, the choice of the right staff and enrollment from third-party pattern. Five other authorization patterns have been described; Reference Monitor, Access Matrix Role authorization rule, and Role-based access control, Remote Authenticator / Authorizer and File Authentication Patterns

4.12 Attack Graph - based Vulnerability Assessment of Rank Property in RPL-6LOWPAN in IoT [24]:

This paper investigates the vulnerabilities of the rank property of RPL (Routing Protocol over Low power and Lossy network) by constructing an attack graph. In the attack graph they analyzed all the possible threats associated with rank property (Table. 1). The investigation showed that violation of protocols related to rank property results in several RPL attacks causing topological sub-optimization, topological isolation, resource consumption and traffic disruption. Also, authors presented some observations, which can be used to devise mechanisms to prevent the exploitation of the vulnerabilities of the rank property.

Table 1: [24] Impacts of Rank Attacks on Network Performance

Attack Type	No of Control Messages	Average Power Consumption	Avg. Beacon Interval	ETX	Packet Loss	Instigate Other Attacks
Increased Rank Attack	Increases	Increases	Decreases	-	-	Yes
Decreased Rank Attack	-	-	-	Increases	Minimal	Yes
Decreased Rank Attack with SFA	-	-	-	Increases	Huge	Yes
Worst Parent Attack	-	-	-	Increases	-	No

4.13 Security Analysis of an IoT System Used for Indoor Localization in Healthcare Facilities [25]:

This paper aims to analyze what security holes and data leaks LoCATE (Localization of Health Center Assets Through an IoT Environment) creates in a healthcare facility. Authors showed the dangers of using simple and default passwords, the need to physically secure edge nodes, and the importance of securing data before transmission. They exploited the system's weak security measures by forging edge node data, gaining unauthorized access, performing denial of service attack, and launching other attacks. They analyzed the successfulness of these attacks to offer mitigation techniques for future devices located in other critical areas similar to the healthcare facilities. The architecture of the system LOCATE illustrated is illustrated in Fig. 7.

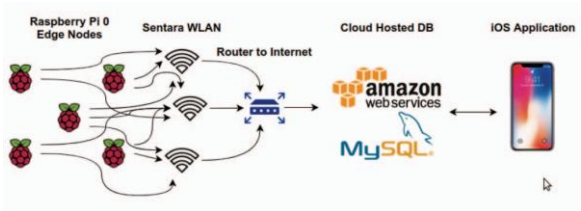

Fig. 7 f25] Architecture Diagram of The LOCATE System

4.14 Security and Privacy Solution for I-RFID based Smart Infrastructure Health Monitoring [26]:

Authors presented an I-RFID (Integrated Radio Frequency Identification) based cellular IoT (C-IoT) system (Fig. 8) and highlighted its key security issue. They proposed an algorithm that, through simulation showed to be secure from various attacks and more useful in the practical scenario for C-IoT network communication in smart infrastructure health monitoring.

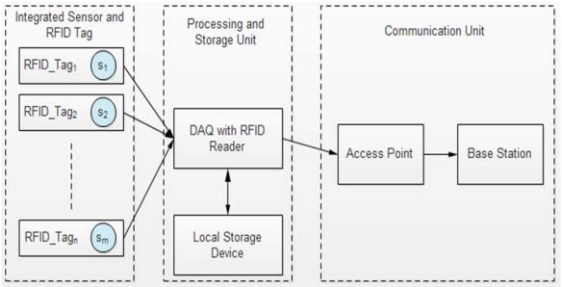

Fig. 8 from [26] System block diagram for integrated-RFID communication process

4.15 Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments [27]:

The authors presented a comprehensive survey of current IoT technologies and security issues with a focus on the Smart Home and City environments. They discussed possible solutions for improving IoT security that focus on today's endpoint device security issues and the anticipated future attacks on data protocols and connectivity.

4.16 Improvement of Security and Scalability for IoT Network Using SD-VPN [28]:

In this paper, authors proposed SD-VPN architecture (Fig. 9) to address the security and scalability issues from the networking perspective. The proposed SD-VPN stated that each IoT application is allocated with its own overlay VPN. They proposed to use the SDN controller to push the flow table of each VPN to the related OpenvSwitch via the OpenFlow protocol. The SD-VPN solution can improve the security of an IoT network by separating the VPN traffic and utilizing service chaining. It also improves the scalability by its overlay VPN nature and the VxLAN technology.

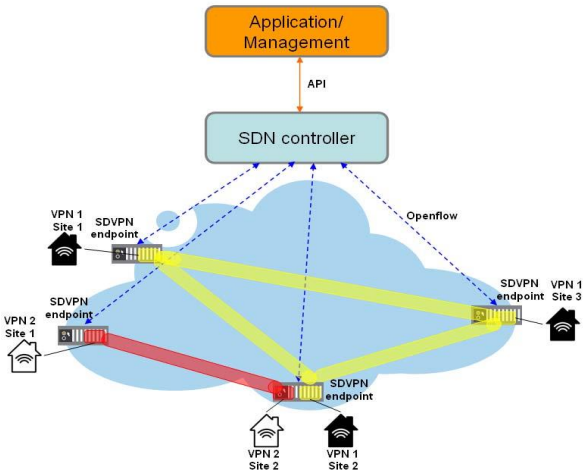

Fig. 9 [28] SD-VPN Architecture

4.17 Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT) [29]:

Authors emphasized on security forensic and its importance against the growth of cyber-attacks. They mentioned the weaknesses of IoT devices security because of the lack of unified standards. Fig. 10 illustrates the forensics process and the application used, and the type of forensics.

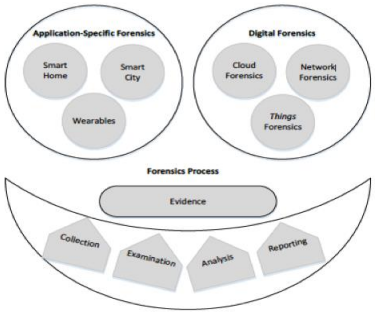

Fig. 10 [29] Application-Specific Digital Forensics Investigation Model in IoT

4.18 Community Guard: A Crowd sourced Home Cyber-Security System [30]:

In this paper, authors presented a community guards system that protects users against malicious traffic attacks. The new solution can be used to protect every home user from DDoS attacks. The prototype mechanism is shown in Fig. 11

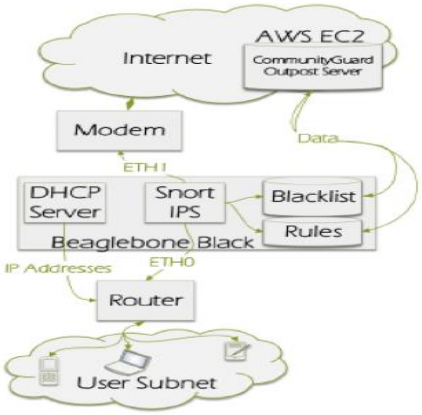

Fig. 11 [30] Prototype Overview

4.19 IoT Security (IoTSec) Mechanisms For e-Health and Ambient Assisted Living Applications [31]:

The paper talked about how IoT touches almost every aspect of our lives, smart cities, transportation, crowdsourcing and E-health. It also talked about the increase of IoT devices around us, and described IoT protocol architecture and examines some of the security tools in IoT.

4.20 Beyond Telnet: Prevalence of IoT Protocols in Telescope and Honeypot Measurements [32]:

The authors talked about the lack of security in the IoT devices, and how many of them would be online with the default credentials which is very dangerous, They deployed three honeypots with 15 IPV4 address, in order to observe the adversary movements and study them, the study showed that the IoT devices were the most targeted for its weak security, especially for DDoS attacks. The targeted protocols were MQTT, CoAP, UPnP, and HNAP. The Fig. 12 shows the most targeted ports in the honeypots.

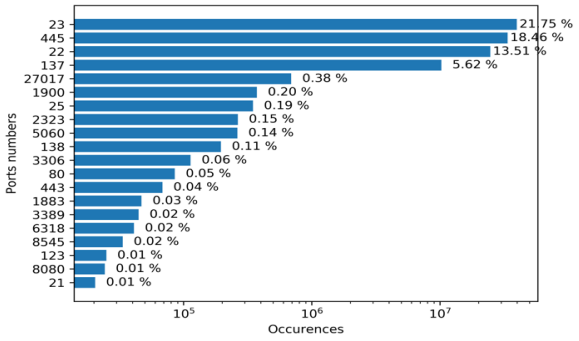

Fig. 12 [32] most ports targeted

4.21 A Secure Event Logging System for Smart Homes [33]:

Authors proposed a secure Host based Event Logging system for smart homes. The solution concentrates on the event logging, and it has 3 layers as shown in Fig. 13, an application layer, a common service layer and a network of things layer. In order to provide the integrity of the system, authors proposed to use Bitcoin Blockchain.

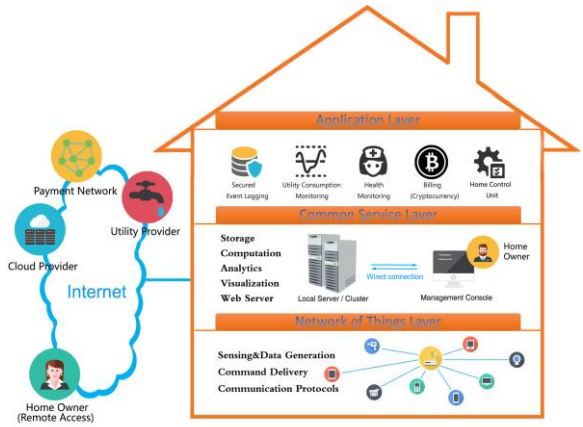

Fig. 13 [34] Three layers framework for Smart home

4.22 Deep Learning and Software-defined Networks: Towards secure IoT Architecture [34]:

With the upraise of the IoT usage among us, the more obstacles we observe through conveying our traditional communication standards against the IoT networking. Since there is no commonly unified standard for the IoT architecture, the authors illustrated the solution of IoT networking based on SDN this is to accommodate the new concepts of scalability and resilience. The authors believe by this incorporation of IoT and SDN you'll be able to improve the network security of IoT by utilizing SDN applications such as detection systems. This comes with a cost of additional risks that are associated with adding a new concept to the mix such as the SDN, where control planes are targeted and vulnerable against attacks. Below is an illustration of the proposed design in Fig. 14.

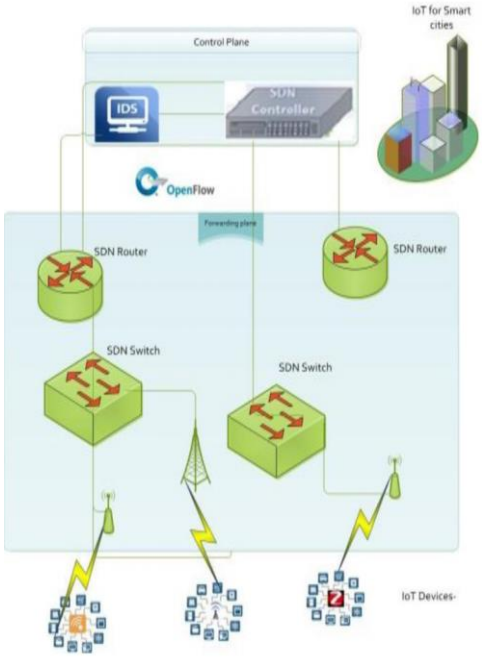

Fig. 14 [35] Proposed Design

4.23 VirtSense: Virtualize Sensing through ARM TrustZone on Internet-of-Things [35]

Authors discussed the limitation of Linux OS running on ARM processors, where you are restricted to use only a single sensing interface in order to ingest the level of traffic or application. They proposed to use a virtualization concept (VirtSense) as shown in Fig. 15 to increase the number of sensing interfaces by balancing the data sensing among multiple interfaces, which allows reducing the complexity of sensors and increasing their usability.

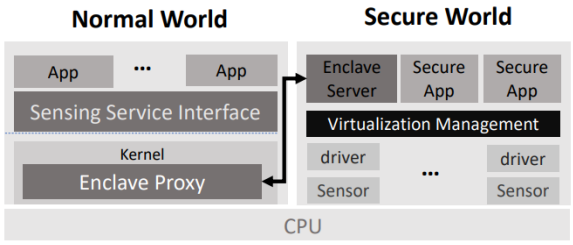

Fig. 15 [36] Overview VirtSense Solution

4.24 Sapphire: Using network gateways for IoT Security [36]:

Authors provided an insight on the employment of network gateways as a NAT that comes between IoTs, local area network (LAN), and the Internet.

Thy proposed a solution called "Sapphire Gateways", which help to get an insight required to monitor and detect suspicious activities locally in the network. They believe that gaining vision on network will efficiently enhance the security along with the implementation of other security requirements such as encryption

4.25 ShieldScatter: Improving IoT Security with Backscatter Assistance [37]:

To counter the attacks targeting IoT devices on the physical layer, author proposed a solution called Authors proposed a "ShieldScatter" as illustrated in Fig. 16. They deployed an antenna device that doesn't rely on battery to run and leverage a lightweight system, thus creating a system that looks like a sphere to protect those devices. By creating a signature profile using signals sampling that is unique to legitimate users; they managed to classify the genuine requests from the fake ones.

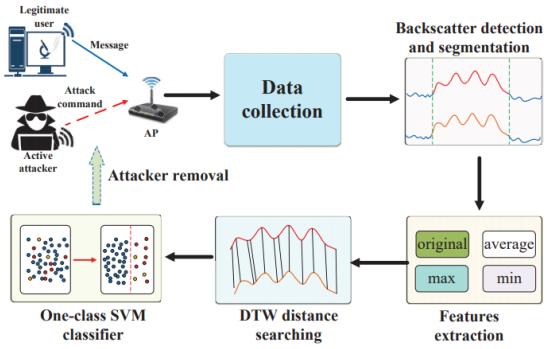

Fig. 16 from [38] ShieldScatter Overview

4.26 Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles [38]:

Due to the constant violations against Internet of things devices in the world through malicious users, botnet attacks and malware, Internet Engineering Task Force (IETF) pushes vendors to the standardization of specifications of IoTs devices to the purpose of manufacturing in the form of Manufacturer Usage Description (MUD). The authors focused on the methods to be done in order to verify the MUD profiles of those IoT devices that will enable smart devices factories to be able to verify the compatibility of their devices with the MUD specifications. Also, it will help to track and analyses any network behavior associated with an IoT device. Fig 17 shows the MUD of Amazon Echo IoT device.

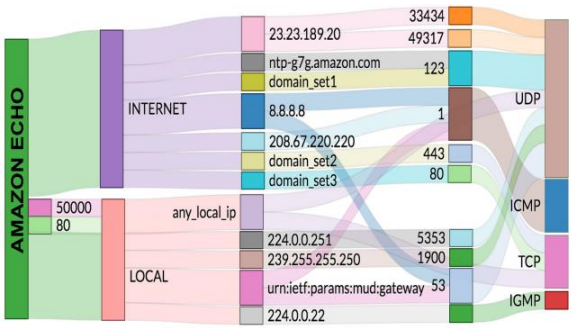

Fig. 17 [39] MUD profile of Amazon Echo

4.27 Combining MUD Policies with SDN for IoT Intrusion Detection [39]:

The authors highlighted the use of the IDS services in SDN to leverage the network flow management where a MUD policy can be tailored to some behaviors. They employed this policy to identify 28 IoT devices that have been connected to a network from different manufacture. In addition, they incorporated other traditional networking IDS policies against those devices with MUD as a profile identifier and they were able to successfully detect different type of attacks that vary from volumetric to spoofing and others. Fig. 18 shows an overview solution of IoT Intrusion detection combining MUD and SDN.

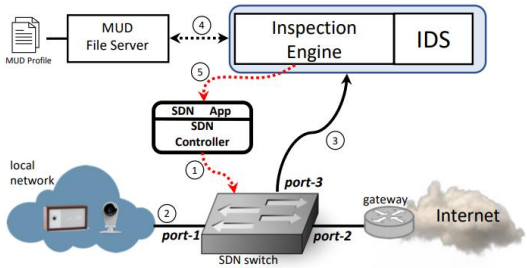

Fig. 18 [40] Overview of combining MUD and SDN for Intrusion Detection

5. IoT Security analysis, trends and Evolution

5.1 Evolution and Trends in IoT Security [40]:

In this paper, authors discussed the evolvement of the IoT field, which as a result impact the security capabilities. They also presented a study of IoT security concerns and an overview of the existing and future trends in this area. Then, they discussed the trends in IOT security and miss-trust in IoT and how to integrate the security controls in the IoT devices.

5.2 Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study [41]:

This paper present a review of recent challenges, trends, and concerns related to IoT security. It discusses three generations of IoT security from past to future. The first generation shared common security practices with general computer usage. The second generation is the current one, Cloud-based centralized IoT service platforms have been welcomed by developers because of their ease of implementation and privacy concerns decreases. The third generation is the future, which focusses on industry and market driven approaches, where more technologies will be involved. Table. 2 summarizes the generations of IoT Security.

Table 2: [42] Three Generation of IoT Security

First generation	Second generation	Third generation
• Used in a test environment • Common security practices: confidentiality, availability, and integrity • Concerns in technology adoption • Data privacy • End-to-end encryption • No standard	• Used in a real environment • More standardized protocol • Centralized IoT service platform • Ease of implementation • Less concerns about privacy • More trust and confidence • Authentication and identification • Single point of failure • Under control	• More industry and market driven • Linking to other technologies • Value creation from big data of customer transactions • Privacy of customers' sensitive data • Replacement of smartphone or BYOD • IoT policy

5.3 Big IoT Data Stream Analytics with Issues in Privacy and Security [42]:

IoT devices today are being used in various applications, which are associated with sensing and control systems. In this paper, authors discussed how data is being collected and moved through the Internet. This big data stream needs to be processed and make it usable, thus privacy is the main concern. To avoid any leakage of information, authors suggested to use hardware based cryptography using Intel technology.

6. Conclusion

From the surveyed papers, IoT devices are exposed to many threats and attacks, which requires unique countermeasures. As the technology burgeons, privacy and security concerns are still going to pose imminent threats. There is room to further the research on the field to establish a model that will guarantee the highest security to all the layers in IoT architecture. However, it is worth to mention that from the surveyed papers we conclude that all the papers neglected to present a robust method of encryption and forensics. In the future, we aim to do a more comprehensive survey emphasizing on encryption and block chain techniques in the IoT field.

References

[1] B. Alsamani and H. Lahza, "A taxonomy of IoT: Security and privacy threats," in 2018 International Conference on Information and Computer Technologies, ICICT 2018, 2018.

[2] Y. Seralathan, T. T. Oh, S. Jadhav, J. Myers, J. P. Jeong, Y. H. Kim and J. N. Kim, "IoT security vulnerability: A case study of a Web camera," in International Conference on Advanced Communication Technology, ICACT, 2018.

[3] Sfar, Arbia, et al. "A Systemic and Cognitive Vision for IoT Security: A Case Study of Military Live Simulation and Security Challenges." International Conference on Smart, Monitored and Controlled Cities SM2C'17, 2017.

[4] Dean and M. O. Agyeman, "A Study of the Advances in IoT Security," in Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control - ISCSIC '18, 2018.

[5] Vashi, Shivangi, et al. "Internet of Things (IoT): A Vision, Architectural Elements, and Security Issues." I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference On, IEEE, 2017, pp. 492–496.

[6] Ahemd, Mian Muhammad, et al. "IoT Security: A Layered Approach for Attacks & Defenses." Communication Technologies (ComTech), 2017 International Conference On, IEEE, 2017, pp. 104–110.

[7] Miettinen, Markus & Sadeghi, Ahmad-Reza. "Keynote: Internet of Things or Threats? On Building Trust in IoT". 1-9. 10.1109/CODESISSS.2018.8525931, 2018.

[8] Y. Seralathan, T. T. Oh, S. Jadhav, J. Myers, J. P. Jeong, Y. H. Kim and J. N. Kim, "IoT security vulnerability: A case study of a Web camera," in International Conference on Advanced Communication Technology, ICACT, 2018.

[9] B. Alsamani and H. Lahza, "A taxonomy of IoT: Security and privacy threats," in 2018 International Conference on Information and Computer Technologies, ICICT 2018, 2018.

[10] Z. Bakhshi, A. Balador and J. Mustafa, "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models," in 2018 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2018, 2018.

[11] Mazwa Khawla and Mazri Tomader. 2018. "A Survey on the Security of Smart Homes: Issues and Solutions,". In Proceedings of the 2nd International Conference on Smart Digital Environment (ICSDE'18), Faissal El Bouanani and Ahmed Habbani (Eds.). ACM, New York, NY, USA, 81-87, 2018.

[12] Glenn Barrie, Andrew Whyte, and Joyce Bell. "IoT security: challenges and solutions for mining," In Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing (ICC '17). ACM, New York, NY, USA, Article 38, 9 pages. DOI: https://doi.org/10.1145/3018896.3018933, 2017.

[13] Oravec, Jo Ann. "Emerging 'Cyber Hygiene' Practices for the Internet of Things (IoT): Professional Issues in Consulting Clients and Educating Users on IoT Privacy and Security." Professional Communication Conference (ProComm), 2017 IEEE International, IEEE, 2017, pp. 1–5.

[14] Kaliya, Neha, and Muzzammil Hussain. "Framework for Privacy Preservation in IoT through Classification and Access Control Mechanisms." 2nd International Conference for Convergence in Technology, 2017.

[15] Adiono, Trio, et al. "Intelligent and Secured Software Application for IoT Based Smart Home." IEEE 6th Global

Conference on Consumer Electronics, 2017.] [Ahemd, Mian Muhammad, et al. “IoT Security: A Layered Approach for Attacks & Defenses.” Communication Technologies (ComTech), 2017 International Conference On, IEEE, 2017, pp. 104–110.

[16] Meng, Weizhi. "Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling". Computer. 51. 36-43. 10.1109/MC.2018.3011034. 2018.

[17] R. Yu, G. Xue, V. T. Kilari and X. Zhang, "Deploying robust security in internet of things," in 2018 IEEE Conference on Communications and Network Security, CNS 2018, 2018.

[18] S. Rizvi, A. Kurtz, J. Pfeffer and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, 2018.

[19] T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," in Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, 2018.

[20] Y. Liu, Y. Kuang, Y. Xiao and G. Xu, "SDN-Based Data Transfer Security for Internet of Things," IEEE Internet of Things Journal, 2018.

[21] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," IEEE Internet of Things Journal, 2018.

[22] Z. Han, X. Li, K. Huang and Z. Feng, "A software defined network-based security assessment framework for cloudIoT," IEEE Internet of Things Journal, 2018.

[23] Ali and M. Asif, "Applying security patterns for authorization of users in IoT based applications," in 2018 International Conference on Engineering and Emerging Technologies, ICEET 2018, 2018.

[24] R. Sahay, G. Geethakumari and K. Modugu, "Attack graph-Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT," in IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings, 2018.

[25] C. Bradley, S. El-Tawab and M. H. Heydari, "Security analysis of an IoT system used for indoor localization in healthcare facilities," in 2018 Systems and Information Engineering Design Symposium, SIEDS 2018, 2018.

[26] S. Kumar, B. Mahapatra, R. Kumar and A. K. Turuk, "Security and privacy solution for I-RFID based smart infrastructure health monitoring," in International Conference on Technologies for Smart City Energy Security and Power: Smart Solutions for Smart Cities, ICSESP 2018 - Proceedings, 2018.

[27] D. Bastos, M. Shackleton and F. El-Moussa, "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments," in Living in the Internet of Things: Cybersecurity of the IoT - 2018, 2018.

[28] L. Shif, F. Wang and C. H. Lung, "Improvement of security and scalability for IoT network using SD-VPN," in IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018, 2018.

[29] T. Zia, P. Liu and W. Han, "Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)," in Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17, 2017.

[30] C. E. Stewart, A. M. Vasu and E. Keller, "CommunityGuard," in Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization - SDN-NFVSec '17, 2017.

[31] Daniel Minoli, Kazem Sohraby, and Benedict Occhiogrosso.”IoT security (IoTsec) mechanisms for e-health and ambient assisted living applications.” In Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE '17). IEEE Press, Piscataway, NJ, USA, 13-18, 2017.

[32] L. Metongnon and R. Sadre, "Beyond Telnet: Prevalence of IoT Protocols in Telescope and Honeypot Measurements," in Proceedings of the 2018 Workshop on Traffic Measurements for Cybersecurity - WTMC '18, 2018.

[33] S. Avizheh, T. T. Doan, X. Liu and R. Safavi-Naini, "A Secure Event Logging System for Smart Homes," in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy - IoTS&P '17, 2017.

[34] A.Dawoud, S. Shahristani and C. Raun, "Deep learning and software-defined networks: Towards secure IoT architecture," Internet of Things, 2018

[35] R. Liu and M. Srivastava, "VirtSense: Virtualize Sensing through ARM TrustZone on Internet-of-Things," in Proceedings of the 3rd Workshop on System Software for Trusted Execution - SysTEX '18, 2018.

[36] Paul Giura and Trevor Jim. “Sapphire: using network gateways for IoT security.”, In Proceedings of the 8th International Conference on the Internet of Things (IOT '18). ACM, New York, NY, USA, Article 5, 8 pages, 2018.

[37] Z. Luo, W. Wang, J. Qu, T. Jiang and Q. Zhang, "ShieldScatter: Improving IoT Security with Backscatter Assistance," in Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems - SenSys '18, 2018.

[38] A.Hamza, D. Ranathunga, H. H. Gharakheili, M. Roughan and V. Sivaraman, "Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles (Technical Report)," 2018.

[39] Hamza, H. H. Gharakheili and V. Sivaraman, "Combining MUD Policies with SDN for IoT Intrusion Detection," in Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P '18, 2018.

[40] R. Roman-Castro, J. Lopez and S. Gritzalis, "Evolution and Trends in IoT Security," in Computer, vol. 51, no. 7, pp. 16-25, 2018.

[41] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew and H. Dang Hai, "Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study".

[42] L. Khan, "Big IoT Data Stream Analytics with Issues in Privacy and Security," in Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics - IWSPA '18, 2018.

Ahmed Redha Mahlous received his MSc in Computer Systems and Internetworking from South Bank University (London, UK) and a PhD degree in Computer Networks from University of Bradford (UK). His area of research includes Network Security, Software Security and QoS. He is currently working as an assistant professor at Prince Sultan University (Riyadh, KSA).