2020 IEEE Workshop on Emerging Technologies for Security in IoT (ETSecIoT)

IoT Threat Detection Advances, Challenges and Future Directions.

Nickson M. Karie
Cyber Security Cooperative Research Centre
Edith Cowan University
Perth, Australia
nickson.karie@cybersecuritycrc.org.au

Nor Masri Sahri
Cyber Security Cooperative Research Centre
Edith Cowan University
Perth, Australia
masri.sahri@cybersecuritycrc.org.au

Paul Haskell-Dowland
Cyber Security Cooperative Research Centre
Edith Cowan University
Perth, Australia
ORCID: 0000-0003-1365-0929

***Abstract*—It is predicted that, the number of connected Internet of Things (IoT) devices will rise to 38.6 billion by 2025 and an estimated 50 billion by 2030. The increased deployment of IoT devices into diverse areas of our life has provided us with significant benefits such as improved quality of life and task automation. However, each time a new IoT device is deployed, new and unique security threats emerge or are introduced into the environment under which the device must operate. Instantaneous detection and mitigation of every security threat introduced by different IoT devices deployed can be very challenging. This is because many of the IoT devices are manufactured with no consideration of their security implications. In this paper therefore, we review existing literature and present IoT threat detection research advances with a focus on the various IoT security challenges as well as the current developments towards combating cyber security threats in IoT networks. However, this paper also highlights several future research directions in the IoT domain.**

Keywords—IoT, threat detection, challenges, future directions.

I. Introduction

We live in an era where technology is a necessity to every human being. This is evident from the increased reliance on technology in almost everything we do [1]. This has thus led to the exponential growth of IoT devices use in different areas of our life such as supply chain, health care, vehicular networks among other areas, which is also slowly reaching its critical mass and becoming a reality in our daily life. While IoT devices can improve the quality of life, task automation and productivity by making it possible to access data anytime and anywhere, the threat level introduced in organisations as a result of these devices is alarming. Access to data and information, for example, can bring significant security threats challenges to a network by introducing viruses which can have devastating effects on the operations of an organisation. This scenario shows that IoT devices can be used for both good and bad activities, hence, significant research on IoT security threat detection and challenges can help shape the future of the IoT domain.

Again, knowing that each time a new IoT device is deployed, new and unique security threats may be introduced into the environment under which the device must operate, protecting IoT networks therefore calls for further research and development of various lightweight security protocol to enhance the security of any communication between different IoT devices in the network. This is backed up by the fact that, the implementation of any IoT architecture in conventional networks requires several modifications because many of the IoT devices used may often be manufactured with no consideration of their security implications.

The lack of standards in the manufacture of IoT devices sometimes makes it possible for sophisticated IoT attack vectors to go undetected in IoT networks. For this reason, potential threats in the domain has grown dramatically, but at the same time, a great number of threats mitigation measures have also been researched on significantly. The aim of this paper, therefore, is to present IoT threat detection advances as well as the current developments towards combating cyber security threats in IoT networks. However, this paper also highlights several IoT security challenges and make mention of future research directions in the IoT domain. A review of the current IoT threat detection advances, challenges and a mention of the future directions is the main contribution of this paper.

The rest of the paper is structured as follows: Section II presents a brief IoT background while Section III explains the current IoT threat detection research advances. The IoT challenges are discussed in Section IV followed by the future research directions in Section V. Finally, conclusions are given in Section VI.

II. IoT Background

IoT can be considered as a global distributed network of physical objects that are capable of sensing or acting on their environment, and able to communicate with each other as well as other machines or computers [2]. IoT tries to connect things or objects together either through wired or wireless connections to enable the collection and exchange of data and information that have never been possible before [3]. This also implies that, with IoT many things, objects or sensors can be connected through communications and information infrastructure to provide value-added services to different areas of an organization [2]. Depending on the use case, IoT may also present other benefits and value to organizations such as cost savings, improved revenues, task automation as well as opportunities to continuously innovate [4]. In addition, IoT can also open huge opportunities for both individuals and national economies to explore.

However, for one to use IoT effectively, the different IoT components must be meshed perfectly as part of a well-thought-out structure which forms the basis of any IoT architecture. In this context, irrespective of the use case, most IoT solution architectures will incorporate the same basic or fundamental components which include, the IoT devices or sensors, connectivity, IoT platform and finally the IoT applications. With advances in technology though, some modern IoT solution architectures may include additional layers on top of the four basic components mentioned.

978-1-7281-8019-9/20/$31.00 ©2020 IEEE
DOI 10.1109/ETSecIoT50046.2020.00009

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.

Note that, because of the dynamic nature of the new technologies being introduced into the IoT domain on a daily basis, it has become very hard for anyone to have a single reference architecture that can be used as a blueprint for all possible concrete implementations [5]. For this reason, several reference architectures coexist in the IoT domain. Besides, according to [6] there is no single universally agreed consensus on IoT architecture hence, the reason why different solution architectures have been proposed by different researchers. Figure 1 below shows how the basic IoT components can be connected to each other to provide simple IoT solutions.

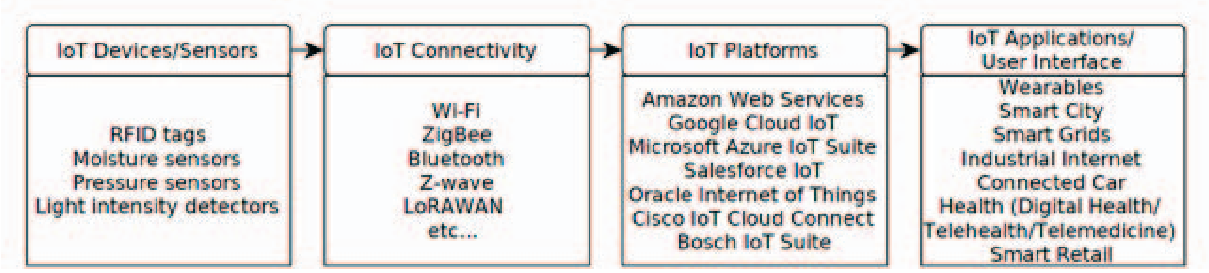

Figure 1: Basic IoT Components.

Infer from Figure 1 that, the IoT devices/sensors include the physical hardware components intended to suite a specific IoT solution. Different IoT solutions will require different hardware devices. Whatever the case, the devices will always need to send data to and receive commands from some centralized IoT platform. One thing to note at this point is that the device-to-platform connection options (wired or wireless) will depend heavily on the environment under which the device must operate and constraints of the device itself. In the case where a device can't connect directly to the available platform, an IoT gateway may be used to bridge the gap between the local environment and the platform to be used. The IoT devices are then connected to the gateway which then reads the required information and then sends the data to the platform using an existing IoT connection, which can access the existing network or the available platform [7].

While it can be very hard to discuss all the IoT components details as well as the possible IoT architectures that exist in the market today, the following categories in the next sub-sections cover the most basic and mostly used IoT architectures.

A. Three Layer IoT Architecture

This architecture is considered to be the very basic IoT architecture that exist [8] and has three fundamental building blocks namely, the perception layer, network layer and the application layer as shown in Figure 2.

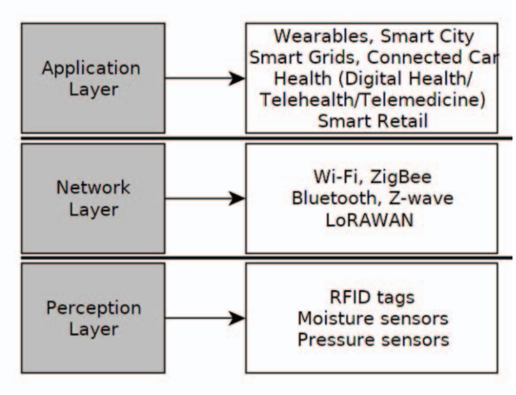

Figure 2: Three-layered IoT Architecture.

The perception layer takes care of the IoT devices or sensors as shown in Figure 1. The devices are capable of interacting with the environment under which they must operate. The perception layer is tasked with the responsibility of identifying things and collecting information from them [8].

The network layer on the other hand which acts like a bridge between perception layer and application layer. It is tasked with the IoT connectivity which connects and translates the IoT devices over a network. Finally, the application layer defines all applications that use the IoT technology, for example, smart homes, smart cities, smart health among others.

B. Four Layer IoT Architecture

Because of the limitations of the three-layer IoT architecture and the advances in IoT technology a four-layer IoT architecture was proposed by [9]. On top of the three layers discussed earlier on the three-layered IoT architecture one fourth support layer was added to take care of security matters. With the addition of the fourth layer, the functionality of the other three layers remain the same as those in the three-layer architecture. Figure 3 below shows the four-layered IoT architecture.

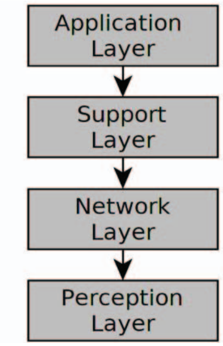

Figure 3: Four-layered IoT architecture

As shown in Figure 3, the support layer was mainly introduced for two main reasons. First to confirm that information is always sent by authentic users (authentication) and protected from security threats.

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.

The second task is sending the information to the network layer [8].

C. Five Layer IoT Architecture

The five-layer IoT Architecture was also built on top of the three-layer architecture approach. Because of security and storage concerns experienced in the four-layer architecture, a five-layer IoT Architecture was proposed [10, 11, 12]. In this Architecture, two more layers, a Business Layer and a Processing Layer were added. The business layer was introduced to manage the entire IoT system, its functionality, applications, and business models while the processing layer handles the analysis, storage, and processing of large data sets. Figure 4 below shows the five-layered IoT architecture.

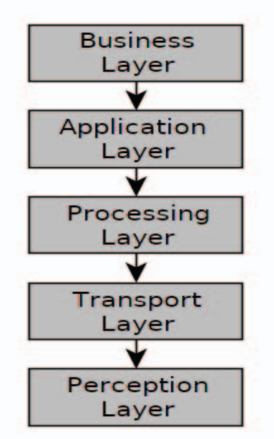

Figure 4: Five-layered IoT architecture

D. Other Proposed IoT Architectures in use

Besides the above discussed IoT architectures, there are other proposed architecture by different researchers as shown in the bulleted list below. Note again that the list provided here is not comprehensive as new IoT Architectures keep emerging based on individual use cases. Some of the newer conventions include:

- Fog Computing IoT Architecture
- Edge Computing Architecture
- Cloud and Fog Based Architectures
- Cloud-Fog-Edge Architecture
- Mist Computing Architecture
- S-IoT (Social IoT) Architecture
- IoT-A Architecture

The next section investigates the current research advances in IoT threat detection mechanisms.

III. Current Research Advances in IoT Threat Detection

Data availability in an IoT environment is a major requirement, as many analytical and strategic decisions are made based on data generated in the IoT domain in real time. This section, therefore, provides details of various threat detection techniques categorized by the types of attacks targeting IoT network and devices. Different research approaches have been undertaken by different researchers to find the best methods to handle intrusion detection in IoT [13].

To protect IoT devices against cyber security threats such as Man-In-The-Middle (MITM) and Distributed Denial of Service (DDoS), for example, Kabir et al. [13], proposed an approach for an intrusion detection system based on sampling with Least Square Support Vector Machine (LS-SVM).

On the same note, Ahmed and Rajput [14] researched on protecting IoT infrastructure from Distributed Denial of Service (DDoS) attacks. In their work, a Naïve Bayes classification algorithm is utilized in their developed Intrusion Detection Systems (IDSs). A multi agent systems which consists of a set of autonomous agents that can work together to learn and share experiences among IoT devices is applied in their proposed solution. Multi agent IDSs are then deployed in the network to sense the abnormal or misbehaving traffic between the nodes involved in the communication. Four types of agent are used in the distributed routers cooperating with each other. The *collector agent* is responsible for data collection from the network. The *system monitoring* agent monitors the whole structure of multi agents deployed and its main objective is to classify the data to determine whether the data is normal or indicative of an attack. An *actuator agent* is created to react to the detected intrusions and could drop the connectivity of the potential attacker. Finally, the *communication agent* is developed to share results of detection information with other agents in the network. The developed solution provides faster reporting of detection and prevention of attacks and the total load is well distributed among all participate agents in the network.

Another research by Mehmood et al. [15] describe how IoT specific network behaviours are used to inform feature selection to improve the accuracy of attack detection. The objective of the work is to detect and prevent Denial-of-Service (DoS) attack traffic originating from devices in the home network. Machine learning algorithms that perform data collection, feature extraction and binary classification for IoT traffic Distributed Denial-of-Service (DDoS) detection was developed as part of the proposed solution. To detect the anomaly in IoT, the authors assume that IoT traffic is different from other types of network behaviour. The author claimed that IoT activity is more predictable since the devices tend to have a fixed number of network states. Four anomaly detection pipelines are developed. First, records of traffic sent from smart home devices are captured. Then, timestamps recorded from each of the devices are grouped together. Packet header fields and aggregate flow information is extracted to be fed into multiple selected machine learning algorithms for binary classification. From the results, the author achieved approximately 91-99% detection accuracy.

Doshi et al. [16] present a novel anomaly detection method that extracts behaviours of the network and utilize statistical analysis to detect abnormalities originating from compromised IoT devices. Nine commercial IoT devices were intentionally infected with two widely known IoT-based botnets, Mirai and BASHLITE. The raw network traffic was captured using a mirroring port in the switch where the network traffic typically flows. 115 traffic features were extracted from the network level packet information. A neural network autoencoder was used to maintain a model for each of the IoT device separately. Finally, the anomaly threshold was defined as the sum of the sample mean and the standard deviation was calculated from the samples taken in the previous process. The proposed method achieved 100% True Positive Rate (TPR) and raised few false alarms.

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.

More research by Sharma et al. [17] described a distributed Software Defined Networking (SDN) architecture for IoT by integrating SDN and blockchain, allowing nodes to interact with each other without relying on the central controller. For efficient communication between controllers in the IoT environment, all IoT controllers are interconnected in a distributed blockchain manner. Flow control analyser and packet migration components is composed to take care of the main function of the network infrastructure as soon as the attack is started. The authors claim that the proposed solution can identify every attack quickly. Several attack simulations on IoT devices such as ARP poisoning, DDoS and fake topology attacks have been undertaken to measure the accuracy of attacks when these methods are used together in detection. With the proposed technique the attack window time detection is reduced thus allowing faster network attack mitigation.

Nguyen et al [18] presented a collaborative and intelligent network-based IDS for SDN-based cloud IoT. To stop malicious traffic as quickly as possible, a hierarchical layer of intelligent IDS nodes to detect anomalies and formulate policy into the SDN-based IoT gateway devices are composed. Multiple IDS with different function and computing level is purposely located at the edge of the network and on the cloud with enough computation and storage resources for collaborative attack detection. Each of the IDS levels adopt machine learning algorithms such as Support Vector Machine (SVM) and Self Organize Map (SOM) to be used as the classification for the anomaly detection and policy making processes at each level of the network. 30,000 data samples are extracted from three different data sets with extensive TCP and ICMP features. From the performance evaluation, the proposed collaborative IDS architecture guarantees a good level of anomaly detection accuracy in comparison with centralized solutions.

An intrusion detection scheme for routing attacks in IoT environments was proposed by [19]. In routing attack, malicious IoT sensors have the capability to deviate and disrupt the normal flow of traffic. Each of the malicious sensors send packets to its neighbour collaborator attacker node. In this case, the edge node does not receive the intended information. The proposed detection mechanism is performed in two phases. In phase 1, a list of suspected attacker nodes is captured if these suspected nodes are present in the network. The suspected attacker is identified if the level of remaining energy of the IoT sensor is less than current computed energy (drained battery). Then in phase 2, specially crafted status and data query messages are used to determine whether the IoT sensor is an attacker or not. If it does not receive any response from previously sent query messages, then it is assumed that the IoT device is an attacker node.

DDoS attack detection and mitigation using SDN was proposed in [20]. Specific features of IoT traffic are taken into consideration and the proposed solution utilizes edge computing by putting the detection and mitigation job to Openflow switches. A distributed anomaly detection approach provides fast detection and response to IoT based attacks in real time and most importantly it does not overburden the centralized controller. The detection request is processed by the edge gateway without the need for the controller to intervene, thus allowing requests to be processed in real time. Flow level features are employed for the feature extraction process. The experiment is simulated using Mininet which is a frequently used simulator in SDN. Three different machine learning algorithms were chosen for the test to distinguish legitimate flows from DDoS flows. From their experiment, the Random Forest algorithm outperformed the other two machine learning approaches with almost 100% True Positive.

SDN, machine learning and fog computing technology is adopted in another proposed anomaly detection solution by [21]. The framework provides network control in cloud and network edge infrastructure. Comparative parameters for computation at cloud versus network fog for IoT network is devised. Several features are chosen for the machine learning computation. Recurrent Neural Network (RNN), Multi-Layer Perceptron (MLP) and Alternate Decision Tree (ADT) are used to boost the accuracy of detection of DDoS attacks. For the mitigation strategy, each controller maintains an access list that comprises of blacklist prefixes. The authors conclude that fog computing provides better attack detection results compared to cloud infrastructure.

A blockchain-based decentralized security framework for IoT network is proposed in [22]. Three core technologies of SDN, blockchain and fog computing are utilized for more efficient attack detection in IoT networks. SDN is utilized for the ability to continuously monitor and analyse the whole IoT network. Meanwhile, Ethereum blockchain technology provides decentralized detection of the attack to mitigate the problem of "single point of failure" inherent in the current architecture. Fog and mobile edge computing facilitate detection of attacks at the fog node and subsequently attacks at the edge node, allowing early detection and mitigation with lower storage constraints, cheaper computation and low latency. Deep learning algorithms are used for attack detection and subsequently mitigate attack at the edge network. The novel task of dynamic update of detection model provide the ability to have more efficient detection. Numeric, binary and nominal data is fed into the chosen anomaly classifier. Evaluation results show that the proposed decentralized protection model outperforms the centralized and distributed architecture and takes less time to mitigate attacks in the IoT ecosystem.

Intra and inter-domain DDoS mitigation using a blockchain-based approach is proposed in [23]. The scheme allows multiple SDN-based domains to collaborate securely and information about the attacks to be transferred in a decentralized manner. By doing this, it allows an effective attack mitigation near to the source of the attack. By effectively reducing the cost of forwarding packets which are mostly useless attack traffic and an ability to block the attack close to its source, the proposed collaborative approach can mitigate DDoS attacks more efficiently. To realize a decentralized secure solution, the author proposes a smart contract-based approach that makes use of the Ethereum smart contract technology. Furthermore, to measure the randomness of data inside the domain, the flow sampling method is used. Finally, a Bayes-based scheme is used to automatically detect the traffic anomalies inside the domain. From the experimental results, the proposed solution achieves cost effectiveness, efficiency and flexibility in detecting anomalous flows.

Many more approaches have been proposed, and the reader is encouraged to explore more literature beyond what we have managed to survey, for example, Brown et al. [24] presented a survey of Intrusion Detection Systems (IDS) in the IoT domain while Kelton et al. [25] presented a research on

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.

Machine Learning techniques applied in IoT and Intrusion Detection for computer network security. Karsligil et at [26] also presented a semi-supervised anomaly detection system using k-means algorithm while Arrington et al. [27] went ahead to propose a behavioural modelling intrusion detection system (BMIDS) using IoT behaviour-based anomaly detection via immunity-inspired algorithms.

Based on these approaches, Table 1 summarizes the different IoT attacks against each identified countermeasure. It can clearly be seen that most of the researcher is moving toward the use of newly introduced network architecture which is based on SDN network. With the centralize view of an organization entire network, provisioning and streamline enterprise management become much easier for the administrator to defence against cyber threat. The ability to direct and automate decision provide seamless experience for threat detection problems in IoT. The IoT make up from our devices and services creates a substantial amount of data. The question is how we treat, connect, analyse and store all these valuable data? With the use of fog computing technology, the efficiency of managing the amount of data generated from IoT devices is increased efficiently and the amount of data sent to cloud for processing or storage is reduced significantly. Instead of a centralised location that may become vulnerable, there is communication between different local endpoints, making it easier to detect threats such as compromised files, possible hacks or malware. Therefore, the risks are detected much earlier and can be managed at device level rather than infecting or damaging the entire network.

The next section elaborates on the IoT challenges in the modern era.

TABLE I. SUMMARIZED IOT ATTACK IN EACH IDENTIFIED COUNTERMEASURE APPROACH

Attacks	**Technology Used**					***Detection Approach***	***Countermeasure***
	Blockchain	***SDN***	***Fog Computing***	***Traditional Internet***	***Edge Computing***		
DDoS				X		Intrusion detection system, multi agents deployed in the network	[15] multi agent, Naïve Bayes algorithm
				X		IoT devices packet header fields and aggregate flow is used in behaviour learning	[16] using Machine Learning to automatically classify the attacks
		X			X	Machine learning is used to distinguish the IoT-based DDoS attacks.	[20] multiple point defence mechanism is deployed (IoT gateway as IDS)
		X	X			Entropy based algorithm is use for better accuracy detection	[21] anomaly detector is implemented in cloud infrastructure and at the fog computing
	X	X	X		X	Host-based, time-based, content and basic features is used for classification	[22] dynamic update of attack detection model enables efficient attack detection
	X	X				Bayes-base scheme for anomaly detection	[23] Inter and intra-domain collaborative DDoS mitigation
Scanning attacks	X	X				Traffic statistic obtain form packet context summarizes all traffic	[[17] Mean and standard deviation technique is used to classify the attacks
Reconnaissance attacks	X	X	X			Machine learning is use for attack classification	[18] multiple IDS located on the network (edge, fog and cloud IDS)
Routing attacks					X	Remaining energy amount of an IoT sensor is used as the indicator for malicious device	[19] IDS function is placed at the edge based IoT environment

IV. IOT CHALLENGES IN THE MODERN ERA

The IoT ecosystem is a mixture of devices and services that allow for data and information exchange between people and devices, devices and other devices, devices and objects and many other elements and their interactions via the Internet. This simply implies that, everything and anything in the world can be adjusted somehow to connect to the Internet and become part of the global network.

The good thing about IoT is that, once deployed, it has the power to collect and communicate data and information from anything and anyone without human intervention. With this power however comes many risks and challenges that can potentially impact many areas of our daily life. Some of the key challenges of this era are briefly discussed in the next subsections.

A. Privacy Challenges

With the growing number of connected devices in the world, hackers have found many entry points into organization networks. This means that every new IoT device connected to the network has a potential risk of being hacked. Coupled with the power to collect and communicate data and information from anything and anyone without human intervention, IoT devices leave sensitive data and information vulnerable.

Some IoT devices require users to agree to terms and condition of service before using them. These types of agreements can expose users' data making it vulnerable to

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.

attack. As stated by Banafa [28], strategies need to be developed to handle people's privacy options across a broad spectrum of expectations. This, however, must be done in such a way that it can still promote new technological innovations and services while avoiding putting users' private data and information in danger.

B. Security Challenges

Security is the major concern in IoT and includes issues such as authentication, confidentiality, end-to-end security, transparency and capability. Most IoT devices deployed in organisations' networks are vulnerable to cyber-attacks due to their constrained computational resources. This makes it hard to install traditional protective mechanisms like antivirus or firewall tools in them resulting in information breaches or even infiltration. Different IoT devices are manufactured by different vendors running different organisational principles and standards. For this reason, maintaining a consistent level of security across all manufactured IoT devices becomes technically hard. One vulnerable IoT device can allow attackers to manipulate data or information stored within the IoT platform. This therefore shows that; alternative security methods need to be designed in order to secure IoT devices [29].

Besides, IoT application data owned by consumers, industrial or enterprise should be secured against potential threats such as data theft and tampering attempts. Since IoT devices may also store currents and historical user data, their behaviour and finances information, a strong protection mechanism tailored to IoT infrastructure is desired. This is because IoT data is transmitted across the Internet that is widely open to potential cyber threats. IoT application level threat detection such as unique DDoS attack and mitigation strategy should be implemented to help reduce potential risks. Authentication methods such as multi-factor authentication may also be used to confirm the identity of entities that request access to any data or information.

Because of the limitations of power capabilities and computational ability of IoT devices, lightweight security solution has become a necessity. It is not a target in itself, but rather a constraint that must be taken into consideration when developing and enforcing protocols to encrypt or authenticate data and devices in IoT. Since the security algorithms are intended to run on IoT devices with limited capabilities, the system specifications must be compatible. The process of identification and authentication of IoT devices is mainly a challenge because of the nature the devices and the algorithms to be used. Many factors such as people, services, devices and service providers are involved in the process and need to be taken as consideration before any development of an IoT security or protection mechanism.

An attacker might tamper with IoT devices physically since it might be deployed in a remote area and left unattended. Following this, the attacker can then proceed to do harmful activities on the devices such as modify the programs, extract information or even replace them with malicious devices. One way to be employed as a security measure to defend such devices is by having tamper resistant packaging for better protection. With the introduction of different kind of protocols that have been used by IoT devices across the Internet, these multi-protocol characteristics make traditional security protection scheme not suitable for IoT devices. Furthermore, IoT devices can join and leave a network at anytime from anywhere. With the dynamic nature of the network topology, existing security protection do not easily cope with this type of sudden topological changes. With the rapid escalation in the use of IoT devices over the internet an extensive and scalable security solution is urgently needed.

C. Standardization Challenges

From manufacturing to collection and storage of data, IoT devices have no well-structured international standards to be used by stakeholders. With many IoT devices handling unstructured data, unlike structured data which can be stored in relational databases and queried through SQL, unstructured data are stored in different types of NoSQL databases without a standard querying approach [28]. To protect users and enhance security and privacy in IoT, stakeholders should determine effective IoT standards for the next generation IoT devices. Without proper regulation, well defined guidelines and universal standards, the industry will continue to suffer from unregulated IoT sprawl [30].

In addition, with the IoT industry still unproperly regulated there continues to be privacy and security implications. The growing popularity among end users and extensive use of IoT devices in each industry area has created a new attack vector. Similar attacks have resulted in increased recognition of the need for legislation, stronger protection measures and more stringent controls on the authentication of Internet-connected devices [31].

D. Integration Challenges

With the lack of effective standards in the IoT domain, comes integration challenges. As indicated by [32] unacceptable integration can lead to irregularity in working and efficiency in value delivery to the stakeholders. Integration among IoT devices is tightly constrained due to dissimilarities in languages, components, together with hardware and software involved in the IoT device development. In an ideal world, resources can easily fit together to assist compatibility and knowledge exchange. However, communication interoperability is particularly challenging due to the wide range of available technologies making it a challenge to communicate seamlessly between multi-vendor devices. There are some attempts in the market, but the proposed solutions are constrained by the limited number of compatible devices. Therefore, standards which include interoperability among IoT devices are urgently needed.

E. Connectivity Challenges

Recent research has shown that the number of connected devices will rise to 38.5 billion by 2020, up from 13.8 billion in 2015 [33]. This means, managing such a huge number of IoT devices may require restructuring of the existing communication models and the underlying technologies [28]. This is because many existing organizations are used to the centralized, client/server architecture in managing different network nodes. However, with the IoT ecosystems with over 38.5 billion devices in use, the client/server architecture can be a challenge. New communication models to manage IoT devices are thus inevitable with future IoT networks. Some of the suggested paradigms that can be deployed include the use of decentralized IoT networks.

F. Regulation Challenges

Because of the diversity in the applications of IoT devices and the jurisdictions under which IoT devices are deployed, a wide range of regulatory and legal questions exist posing a

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.

challenge to users as to what is allowed and not in each jurisdiction. Some of the legal issues surrounding the use of IoT devices include data retention and destruction policies, legal liability for unintended uses of IoT devices, security breaches or privacy lapses [34] among others.

Global regulation, such as rules, processes, protocols, audits, transparency and continuity, is also currently non-existent in the IoT domain, due to the lack of general legislation in the IoT sector. These levels of regulation at industry, national and international level can be extremely helpful in helping organizations with better efficiency and system reliability and in reducing the potential for future errors.

V. Future Directions

The IoT domain is a growing field and if it must change the world in next few years to come then some of the grey areas that exist need to be investigated and solutions identified. Some of the areas that are part of the future directions in the IoT domain can be summarized as follows:

A. *Intelligent Decision Making*

Up until now, many IoT devices have been developed and deployed in many areas of our life, however, challenges remain to help these devices make more intelligent decisions soon. Intelligent IoT devices will have the potential to transform many decision-making processes by integrating artificial intelligence, machine learning and deep learning into the IoT domain. In this case some of the key question that may need to be addressed include:

- How will the IoT devices collect intelligent information for use in decision making?
- How will the collected intelligent information be stored for easy decision making?
- How will the collected intelligent information be used in a secure way?
- How will the decision-making methods or algorithms be applied to the collected intelligent information?
- How will the decision-making methods or algorithms be improved to continue giving intelligent decisions?
- How will every decision result made by IoT devices be evaluated for effectiveness, efficiency and accuracy?

B. *Edge Computing*

The fundamental weakness IoT has is that it adds up devices behind the network's firewall. Securing IoT devices require a lot more of attention. The need to incorporate security elements between the software applications and the network connection which binds to the devices. Edge computing has been suggested to offer the solution for current IoT devices slow data processing behaviour. Faster data processing is desired in all smart devices to have lower latency in IoT device communication. Data processing with Edge Computing is expected to rise for the advancement of IoT.

C. *Blockchain Integration*

An extensive range of financial and government processes, consumers and industries are moving towards decentralization and self-governance. With the existing single points of failure, the current ecosystems are open to exploitation and entire systems could fail under DDoS attacks. By integrating the IoT environment with blockchain technology, all communication and exchange of information between devices can be based on an autonomous system. Blockchain technology could provide secure documented transactions with a time-stamped contractual handshake approved between devices. IDC [35] has predicted that by 2021, one-third of retailers and manufacturers will be tracking goods using blockchain in anticipation of regulatory changes, resulting in an increase of delivered product quality up to 20%.

D. *Improved/Better Security*

With advances in IoT, more security challenges will be introduced. Research must be done to find new ways of embedding security into the entire IoT ecosystem. This means from the sensor/actuator level to the backend analytical engines; security should be given priority.

VI. Conclusion

IoT has emerged as one technology that has great potential to change the world in many ways. However, this technology threatens users' privacy and security in the different environments under which it must be deployed. For this reason, solutions to threat detection, intrusion, compromise or misuse in the IoT domain should be developed. This paper has highlighted the current research advances in IoT threat detection and summarized the IoT attacks in each identified countermeasure approach. However, key IoT challenges in the modern era have also been identified and discussed. In conclusion, several areas have been identified to give future direction to researchers who would like to explore this domain further. Some guiding question that may be used include: (1). How well can threat detection be done in the IoT Domain? (2). Can the use of machine learning help improve IoT security and privacy? (3). Can standardization be achieved within the IoT domain?

Acknowledgment

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme

References

[1] Cascio, W. & Montealegre, R. (2016). How Technology Is Changing Work and Organizations. Annual Review of Organizational Psychology and Organizational Behavior. 3. 349-375. 10.1146/annurev-orgpsych-041015-062352.

[2] Pundir,Y., Sharma, N. and Singh, Y. (2016). Internet of Things (IoT): Challenges and Future Directions. International Journal of Advanced Research in Computer and Communication Engineering Vol.5, Issue 3, pp.960-964

[3] Burhanuddin, M. A., Mohammed, A.A., Ismail, R.and Basiron, H.,(2017). Internet of Things Architecture: Current Challenges and Future Direction of Research. International Journal of Applied Engineering Research. ISSN 0973-4562 Vol. 12, Number 21 pp.11055-11061

[4] Negi, Y.S. (2016). Internet of Things (IoT): A vision, future directions & Challenges. Available at: https://www.linkedin.com/pulse/internet-things-iot-vision-future-directions-challenges-negi [Accessed on 22nd January 2020]

[5] Jabraeil Jamali M.A., Bahrami B., Heidari A., Allahverdizadeh P., Norouzi F. (2020) IoT Architecture. In: Towards the Internet of Things. EAI/Springer Innovations in Communication and Computing. Springer, Cham

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.

[6] Sethi,P. & Sarangi, S.R., (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering. Vol. 2017, Article ID 9324035

[7] Cannaday, B., (2019). The Fundamental IoT Architecture. Availabel at: https://www.losant.com/blog/the-fundamental-iot-architecture [Accessed on 3rd March 2020]

[8] Burhan,M., Rehman,R.A., Khan, B. and Kim, BS.,(2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors 2018, 18, 2796; doi:10.3390/s18092796

[9] Darwish, D. Improved Layered Architecture for Internet of Things. Int. J. Comput. Acad. Res. (IJCAR) 2015, 4, 214–223.

[10] Madakam, S., Ramaswamy, R., Tripathi, S. (2015) Internet of Things (IoT): A literature review. J. Comput. Commun, 3, 164.

[11] Khan, R., Khan, S.U., Zaheer, R., Khan, S. (2012)Future Internet: The Internet of things architecture, possible applications and key challenges. In Proceedings of the 2012 10th International Conference on Frontiers of Information Technology (FIT), Islamabad, India, 17–19 December 2012; pp. 257–260.

[12] Sethi, P., Sarangi, S.R. (2017) Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng. 2017.

[13] Kabir, E., Hu, j., Wang, H., Zhuo, G. (2018). A novel statistical technique for intrusion detection systems. Future Generation Computer Systems. Vol.79, Issue 1, pp. 303-318

[14] Ahmed, S., Rajput, A.: Threats to patients privacy in smart healthcare environment. In: Lytras, M., et al. (eds.) Innovation in Health Informatics: A Smart Healthcare Primer. Elsevier, Ams-terdam, The Netherlands (2019)

[15] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, ‘‘NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks,’’ J. Supercomput., vol. 7, no. 10, pp. 5156–5170, 2018.

[16] R. Doshi, N. Apthorpe and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, 2018, pp. 29-35. doi: 10.1109/SPW.2018.00013

[17] P.K. Sharma, S. Singh, Y.-S. Jeong, J.H, Park: DistBlockNet: A distributed blockchains-based secure SDN Architecture for IoT networks, IEEE Commun. Mag. 55 (9) (2017) 78–85.

[18] Nguyen, T. G., Phan, T. V., Nguyen, B. T., So-In, C., Baig, Z. A., & Sanguanpong, S. (2019). SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks. IEEE access, 7, 107678-107694.

[19] M. Wazid, P. Reshma Dsouza, A. K. Das, V. Bhat K, N. Kumar, and J. J. P. C. Rodrigues, “RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment,” International Journal of Communication Systems, 2019, https://doi.org/10.1002/dac.4024

[20] Y. Yang, J. Wanf, B. Zhai and J. Liu (2019), “IoT-Based DDoS Attack Detection and Mitigation Using the Edge of SDN,” Cybersapce Safety and Security, 11th International Symposium, CSS 2019 Guangzhou, China, December 1–3, 2019

[21] Shafi Q., Qaisar S., Basit A. (2019) Software Defined Machine Learning Based Anomaly Detection in Fog Based IoT Network. In: Misra S. et al. (eds) Computational Science and Its Applications – ICCSA 2019. ICCSA 2019. Lecture Notes in Computer Science, vol 11622. Springer, Cham

[22] Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park, BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network, Journal of Network and Computer Applications, Volume 143, 2019, Pages 167-177, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2019.06.019.

[23] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, “Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract,” IEEE Access, vol. 7, pp. 98893–98907, 2019

[24] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, Vol. 84, pp.25-37, ISSN 1084-8045.

[25] Kelton A.P. da Costa, João P. Papa, Celso O. Lisboa, Roberto Munoz, Victor Hugo C. de Albuquerque, (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches, Computer Networks, Vol. 151, pp.147-157, ISSN 1389-1286.

[26] Karsligil, M.E., Yavuz, A.G., Guvensan, M.A., Hanifi, K., Bank, H. (2017). Network intrusion detection using machine learning anomaly detection algorithms 25th Signal Processing and Communications Applications Conference (SIU), IEEE (2017), 10.1109/siu.2017. 7960616

[27] Arrington, B., Barnett, L. Rufus, R. and Esterline, A. (2016) "Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms," 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, 2016, pp. 1-6.

[28] Banafa, A. (2017). Three Major Challenges Facing IoT. Available at: https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html [Accessed on 24th January 2020]

[29] Wei, B. (2019). Modern challenges in store for the Internet of Things. Available at: https://www.information-age.com/modern-challenges-internet-things-123470887/ [Accessed on 23rd Jan 2020]

[30] Caroline Hayes. 2018. The Urban Sprawl of the IoT. (2018). http://eecatalog.com/ arm/2018/04/04/the-urban-sprawl-of-the-iot/

[31] J. Saleem and M. Hammoudeh, "Defense methods against social engineering attacks," in Computer and Network Security Essentials, 2017, pp. 603-618.

[32] Sharma, R. (2019). Top 10 Challenges Enterprises Face in IoT Implementation. Available at: https://www.finoit.com/blog/enterprise-challenges-in-iot/ [Accessed on 23rd Jan 2020]

[33] Gupta, P., (2019). Connectivity Challenges in IoT. (Optimal Connectivity for Connected Devices). Available at: http://flarrio.com/connectivity-challenges-in-iot/ [Accessed on 23rd Jan 2020]

[34] Mitchell, R., (2015) Challenges of the Internet of Things. Available at: https://blog.apnic.net/2015/10/20/5-challenges-of-the-internet-of-things/ [Accessed on 24th Jan 2020]

[35] Simon Ellis et al (2017). IDC FutureScape: Worldwide Supply Chain 2018 Predictions. Available at: https://www.idc.com/research/ viewtoc.jsp?containerId=US43146317 [Accessed on 24th Jan 2020]

Authorized licensed use limited to: University of Dayton Libraries. Downloaded on August 18,2020 at 19:03:11 UTC from IEEE Xplore. Restrictions apply.