MOL2NET, International Conference Series on Multidisciplinary Sciences

USEDAT.NET-09: USA-Europe Data Analysis Trends & Complex Networks Congress, Cambridge, UK-Miami, USA, 2023.

Preliminary Study of The Internet of Things (IoT) and Cyber Security for Predictive Data Analytics

Ajit Singh[a], Prof. Dr. G. P. Gadkar [b], Prasanna Kumar [c], Sudhesh Kumar[d], Prof. Dr. Mimi Sinha [e], Pratyush Kumar Prabhat [f], Prof . Kaushlesh Kumar Singh [g] , Rohit Kumar [h], Prof. Dr. Manish Kumar Singh [i]

[a] Patliputra University, Patna, Bihar, India
[b] Patliputra University, Patna, Bihar, India
[c] Amity University, Patna, Bihar, India
[d] Patliputra University, Patna, Bihar, India
[e] Patliputra University, Patna, Bihar, India
[f] Patliputra University, Patna, Bihar, India
[g] Patliputra University, Patna, Bihar, India
.[h] Magadh University, Patna, Bihar, India
.[i] Magadh University, Patna, Bihar, India

.

Abstract: This paper presents a preliminary study of the relationship between IoT and cyber security in the context of predictive data analytics. The study examines the key security challenges associated with IoT devices and the measures that can be taken to mitigate these risks. The paper also explores the role of predictive data analytics in managing and analyzing data collected by IoT devices and the potential benefits and challenges of this approach. The paper further explores the potential benefits of using predictive data analytics in managing and analyzing data collected by IoT devices. These benefits include the ability to identify patterns and trends in data, optimize resource allocation, and improve decision-making. However, the study also identifies challenges associated with the use of predictive data analytics, such as the need for high-quality data, the complexity of analytics algorithms, and the potential for bias and discrimination. Overall, the paper highlights the importance of addressing cyber security challenges associated with IoT devices in the context of predictive data analytics. The study emphasizes the need for comprehensive security measures to be implemented to protect IoT devices and the data they collect. The paper also highlights the potential benefits of using predictive data analytics in managing and analyzing IoT data but cautions that careful consideration of the associated risks and challenges is necessary. Finally, the study identifies areas for future research, such as the development of more effective security measures and the exploration of new data analytics algorithms and techniques.

Keyword: Internet of Things, Cyber-attack, Security threats.

1. Introduction

The current quick improvement of the Internet of Things (IoT) [1, 2] and its capacity to offer diverse sorts of administrations have made it the quickest developing innovation, with colossal effect on social life and business conditions. IoT has step by step saturated all parts of current human life, for example, training, medicinal services, and business, including the capacity of touchy data about people and organizations, money related information exchanges, item advancement and advertising. The immeasurable dispersion of associated gadgets in the IoT has made tremendous interest for hearty security because of the developing interest of millions or maybe billions of associated gadgets and administrations overall [3–5]. The quantity of dangers is rising day by day, and assaults have been on the expansion in both number and multifaceted nature. Not exclusively is the quantity of potential assailants alongside the span of systems developing, however the devices accessible to potential aggressors are likewise winding up noticeably more advanced, proficient and powerful [6, 7]. Accordingly, for IoT to accomplish fullest potential, it needs insurance against dangers and vulnerabilities [8].

Security has been characterized as a procedure to ensure a question against physical harm, unapproved get to, robbery, or misfortune, by keeping up high secrecy and honesty of data about the protest and making data about that question accessible at whatever point required [7, 9].According to Kizza [7] there is no thing as the protected condition of any question, substantial or not, on the grounds that no such protest can ever be in a splendidly secure state and still be valuable. A question is secure if the procedure can keep up its most extreme inborn incentive under various conditions. Security prerequisites in the IoT condition are not the same as some other ICT frameworks. Along these lines, guaranteeing IoT security requires keeping up the most elevated inborn estimation of both unmistakable items (gadgets) and impalpable ones (administrations, data and information). This paper tries to add to a superior comprehension of dangers and their characteristics (inspiration and capacities) beginning from different interlopers like associations and insight. The way toward recognizing dangers to frameworks and framework vulnerabilities is essential for indicating a powerful, entire arrangement of security necessities and furthermore decides whether the security arrangement is secure against malevolent assaults [10]. And clients, governments and IoT designers should eventually comprehend the dangers and have answers to the accompanying inquiries:

- What are the benefits?
- Who are the important substances?
- What are the dangers?
- Who are the risk performing artists?

- What capacity and asset levels do risk on-screen characters have?
- Which dangers can influence what resources?
- Is the present plan secured against dangers?
- What security instruments could be utilized against dangers?

2. Background

The IoT [1, 2, 11] is an augmentation of the Internet into the physical world for connection with physical elements from the environment. Substances, gadgets and administrations [12] are key ideas inside the IoT space, as portrayed in Figure 1 [13]. They have distinctive implications and definitions among different tasks. Along these lines, it is important to have a decent comprehension of what IoT substances, gadgets and administrations are (talked about in detail in Section 2.1). A substance in the IoT could be a human, creature, auto, calculated chain thing, electronic machine or a shut or open condition [14]. Connection among substances is made conceivable by equipment segments called gadgets [12], for example, cell phones, sensors, actuators or RFID labels, which permit the elements to associate with the advanced world [15]. In the present condition of innovation, Machine-to-Machine (M2M) is the most famous application type of IoT. M2M is presently broadly utilized in power, transportation, retail, open administration, wellbeing, water, oil and different ventures to screen and control the client, apparatus and generation forms in the worldwide business et cetera [5, 16, 17]. As per evaluations M2M applications will achieve 12 billion associations by 2020 and create roughly 714 billion euros in incomes [2]. Other than all the IoT application benefits, a few security dangers are watched [17–19]. The associated gadgets or machines are to a great degree profitable to digital assailants for a few reasons:

Most IoT gadgets work unattended by people, in this manner it is simple for an assailant to physically access them.

Most IoT parts impart over remote systems where an assailant could acquire private data by listening in.

Most IoT segments can't bolster complex security conspires because of low power and registering asset capacities.

2.1 Understanding IoT Devices and Services

In this segment, the fundamental IoT area ideas that are imperative from a business procedure point of view are characterized and grouped, and the connections between IoT segments (IoT gadgets and IoT administrations) are depicted.

2.1.1 IoT Gadget

This is an equipment segment that permits the substance to be a piece of the advanced world [12]. It is likewise alluded to as a savvy thing, which can be a home apparatus, medicinal services gadget, vehicle, building, production line and practically anything arranged and fitted with sensors giving data about the physical condition (e.g., temperature, stickiness, nearness locators, and contamination), actuators (e.g., light switches, shows, engine helped screens, or some other activity that a gadget can perform) and installed PCs [24, 25]. An IoT gadget is fit for speaking with other IoT gadgets and ICT frameworks. These gadgets impart by means of various means including cell (3G or LTE), WLAN, remote or different innovations [8]. IoT gadget characterization relies on upon size, i.e., little or ordinary; versatility, i.e., portable or settled; outside or inward power source; regardless of whether they are associated discontinuously or dependably on; computerized or non-robotized; legitimate or physical items; and in conclusion, whether they are IP-empowered articles or non IP objects. The attributes of IoT gadgets are their capacity to activate as well as sense, the ability of constraining force/vitality, association with the physical world, discontinuous network and versatility [23]. Some must be quick and dependable and give solid security and protection, while others may not [9]. Some of these gadgets have physical insurance though others are unattended. Truth be told, in IoT conditions, gadgets ought to be secured against any dangers that can influence their usefulness. In any case, most IoT gadgets are helpless against outside and inside assaults because of their qualities [16]. It is trying to execute and utilize a solid security system because of asset limitations as far as IoT computational abilities, memory, and battery control [26].

2.1.2 IoT Administrations

IoT administrations encourage the simple coordination of IoT elements into the administration arranged design (SOA) world and additionally benefit science [27]. As indicated by Thoma [28], an IoT administration is an exchange between two gatherings: the specialist co-op and benefit shopper. It causes an endorsed work, empowering communication with the physical world by measuring the condition of substances or by starting activities that will start a change to the elements. An administration gives a very much characterized and institutionalized interface, offering all fundamental functionalities for cooperating with elements and related procedures. The administrations uncover the usefulness of a gadget by getting to its facilitated assets [12].

2.1.3 Security in IoT gadgets and administrations

Guaranteeing the security involves shielding both IoT gadgets and administrations from unapproved access from inside the gadgets and remotely. Security ought to ensure the administrations, equipment assets, data and information, both experiencing significant change and capacity. In this area, we recognized three key issues with IoT gadgets and administrations: information secrecy, protection and trust. Information privacy speaks to a major issue in IoT gadgets and administrations [27]. In IoT setting client may access to information as well as approved protest. This requires tending to two vital angles: in the first place, get to control and approval component and second validation and personality administration (IdM) system. The IoT gadget should have the capacity to confirm that the element (individual or other gadget) is approved to get to the administration. Approval decides whether upon distinguishing proof, the individual or gadget is allowed to get an administration. Get to control involves controlling access to assets by conceding or denying implies utilizing a wide exhibit of criteria. Approval and get to control are essential to setting up a safe association between various gadgets and administrations. The fundamental issue to be managed in this situation is making access control rules less demanding to make, comprehend and control. Another viewpoint that ought to be consider when managing privacy is validation and personality administration. Truth be told this issue is basic in IoT, on the grounds that various clients, protest/things and gadgets need to confirm each other through trustable administrations. The issue is to discover answer for taking care of the character of client, things/articles and gadgets in a safe way. Security is an essential issue in IoT gadgets and administration by virtue of the omnipresent character of the IoT condition. Substances are associated, and information is conveyed and traded over the web, rendering client protection a delicate subject in many research works. Protection in information gathering, and also information sharing and administration, and information security matters stay open research issues to be satisfied. Trust assumes an imperative part in building up secure correspondence when various things convey in an indeterminate IoT condition. Two measurements of trust ought to be considered in IoT: confide in the cooperation's amongst substances, and trust in the framework from the clients point of view [29] According to Køien [9] the dependability of an IoT gadget relies on upon the gadget parts including the equipment, for example, processor, memory, sensors and actuators, programming assets like equipment based programming, working framework, drivers and applications, and the power source. With a specific end goal to pick up client/administrations trust, there ought to be a compelling system of characterizing trust in a dynamic and collective IoT condition.

2.2 Security Threats, Attacks, and Vulnerabilities

Before tending to security dangers, the framework resources (framework parts) that make up the IoT should first be recognized. It is essential to comprehend the advantage stock, including all IoT segments, gadgets and administrations. An advantage is a monetary asset, something significant and delicate possessed by a substance. The essential resources of any IoT framework are the framework equipment (incorporate structures, hardware, and so forth.) [11], programming, administrations and information offered by the administrations [30].

2.2.1 Vulnerability

Vulnerabilities are shortcomings in a framework or its outline that permit a gatecrasher to execute summons, get to unapproved information, as well as direct refusal of administration assaults [31, 32]. Vulnerabilities can be found in assortment of ranges in the IoT frameworks. Specifically, they can be shortcomings in framework equipment or programming, shortcomings in approaches and techniques utilized as a part of the frameworks and shortcomings of the framework clients themselves [7]. IoT frameworks depend on two fundamental segments; framework equipment and framework programming, and both have configuration defects regularly. Equipment vulnerabilities are exceptionally hard to distinguish and furthermore hard to settle regardless of the possibility that the powerlessness were recognized because of equipment similarity and interoperability and furthermore the exertion it take to be settled. Programming vulnerabilities can be found in working frameworks, application programming, and control programming like correspondence conventions and gadgets drives. There are various variables that prompt programming configuration imperfections, including human elements and programming multifaceted nature. Specialized vulnerabilities more often than not occur because of human shortcomings. Consequences of not understanding the necessities involve beginning the venture without an arrangement, poor correspondence amongst designers and clients, an absence of assets, aptitudes, and information, and neglecting to oversee and control the framework [7].

2.2.2 Exposure

Presentation is an issue or slip-up in the framework design that permits an aggressor to lead data gathering exercises. A standout amongst the most difficult issues in IoT is strength against presentation to physical assaults. In the greater part of IoT applications, gadgets might be left unattended and liable to be put in area effortlessly available to aggressors. Such introduction raises the likelihood that an assailant may catch the gadget, extricate cryptographic privileged insights, alter their programming, or supplant them with pernicious gadget under the control of the aggressor [33].

2.2.3 Threats

A risk is a move that makes preferred standpoint of security shortcomings in a framework and negatively affects it [34]. Dangers can start from two essential sources: people and nature [35, 36]. Regular dangers, for example, quakes, sea tempests, surges, and fire could make serious harm PC frameworks. Few protections can be actualized against cataclysmic events, and no one can keep them from happening. Debacle recuperation arranges like reinforcement and alternate courses of action are the best ways to deal with secure frameworks against common dangers. Human dangers are those brought on by individuals, for example, noxious dangers comprising of inside [37] (somebody has approved get to) or outer dangers [38] (people or associations working outside the system) hoping to hurt and upset a framework. Human dangers are arranged into the accompanying:

 Unstructured dangers comprising of for the most part unpractised people who utilize effectively accessible hacking instruments.

Structured dangers as individuals know framework vulnerabilities and can comprehend create and misuse codes and scripts. A case of an organized risk is Advanced Persistent Threats (APT) [39]. Able is a modern system assault focused at high-esteem data in business and government associations, for example, fabricating, money related enterprises and national guard, to take information [40]. As IoT turn into a reality, a developing number of omnipresent gadgets has raise the quantity of the security dangers with suggestion for the overall population. Lamentably, IoT accompanies new arrangement of security danger. There are a developing mindfulness that the new era of PDA, PCs and different gadgets could be focused with malware and helpless against assault.

2.2.4 Attacks

Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost [32]. Attack actors are people who are a threat to the digital world [6]. They could be hackers, criminals, or even governments [7]. Additional details are discussed in Section 3.

An attack itself may come in many forms, including active network attacks to monitor unencrypted traffic in search of sensitive information; passive attacks such as monitoring unprotected network communications to decrypt weakly encrypted traffic and getting authentication information; close-in attacks; exploitation by insiders, and so on. Common cyber-attack types are:

Physical attacks: This sort of attack tampers with hardware components. Due to the unattended and distributed nature of the IoT, most devices typically operate in outdoor environments, which are highly susceptible to physical attacks.

Reconnaissance attacks – unauthorized discovery and mapping of systems, services, or vulnerabilities. Examples of reconnaissance attacks are scanning network ports [41], packet sniffers [42], traffic analysis, and sending queries about IP address information.

Denial-of-service (DoS): This kind of attack is an attempt to make a machine or network resource unavailable to its intended users. Due to low memory capabilities and limited computation resources, the majority of devices in IoT are vulnerable to resource enervation attacks.

Access attacks – unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access attack: the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to IP-connected devices.

Attacks on privacy: Privacy protection in IoT has become increasingly challenging due to large volumes of information easily available through remote access mechanisms. The most common attacks on user privacy are:

1. Data mining: enables attackers to discover information that is not anticipated in certain databases.

2. Cyber espionage: using cracking techniques and malicious software to spy or obtain secret information of individuals, organizations or the government.
Eavesdropping: listening to a conversation between two parties [43].

3. Tracking: A user’s movement can be tracked by the devices unique identification number (UID). Tracking a users location facilitates identifying them in situations in which they wish to remain anonymous.

4. Password-based attacks: attempts are made by intruders to duplicate a valid user password. This attempt can be made in two different ways: 1) dictionary attack – trying possible combinations of letters and numbers to guess user passwords; 2) brute force attacks – using

5. Cracking tools to try all possible combinations of passwords to uncover valid passwords.

Cyber-crimes: The Internet and smart objects are used to exploit users and data for materialistic gain, such as intellectual property theft, identity theft, brand theft, and fraud [6, 7].

Destructive attacks: Space is used to create large-scale disruption and destruction of life and property. Examples of destructive attacks are terrorism and revenge attacks.

Supervisory Control and Data Acquisition (SCADA) Attacks: As any other TCP/IP systems, the SCADA [45] system is vulnerable to many cyber attacks [46, 47]. The system can be attacked in any of the following ways:
1. Using denial-of-service to shut down the system.

2. Using Trojans or viruses to take control of the system. For instance, in 2008 an attack launched on an Iranian nuclear facility in Natanz using a virus named Stuxnet [48].

2.3 Primary Security and Privacy Goals

To succeed with the implementation of efficient IoT security, we must be aware of the primary security goals as follows:

2.3.1 Confidentiality

Confidentiality is an important security feature in IoT, but it may not be mandatory in some scenarios where data is presented publicly [18]. However, in most situations and scenarios sensitive data must not be disclosed or read by unauthorized entities. For instance patient data, private business data, and/or military data as well as security credentials and secret keys, must be hidden from unauthorized entities.

2.3.2 Integrity

To provide reliable services to IoT users, integrity is a mandatory security property in most cases. Different systems in IoT have various integrity requirements [49]. For instance, a remote patient monitoring system will have high integrity checking against random errors due to information sensitivities. Loss or manipulation of data may occur due to communication, potentially causing loss of human lives [6].

2.3.3 Authentication and authorization

Ubiquitous connectivity of the IoT aggravates the problem of authentication because of the nature of IoT environments, where possible communication would take place between device to device (M2M), human to device, and/or human to human. Different authentication requirements necessitate different solutions in different systems. Some solutions must be strong, for example authentication of bank cards or bank systems. On the other hand, most will have to be international, e.g., e-Passport, while others have to be local [6]. The authorization property allows only authorized entities (any authenticated entity) to perform certain operations in the network.

2.3.4 Availability

A user of a device (or the device itself) must be capable of accessing services anytime, whenever needed. Different hardware and software components in IoT devices must be robust so as to provide services even in the presence of malicious entities or adverse situations. Various systems have different availability requirements. For instance, fire monitoring or healthcare monitoring

systems would likely have higher availability requirements than roadside pollution sensors.

2.3.5 Accountability

When developing security techniques to be used in a secure network, accountability adds redundancy and responsibility of certain actions, duties and planning of the implementation of network security policies. Accountability itself cannot stop attacks but is helpful in ensuring the other security techniques are working properly. Core security issues like integrity and confidentiality may be useless if not subjected to accountability. Also, in case of a repudiation incident, an entity would be traced for its actions through an accountability process that could be useful for checking the inside story of what happened and who was actually responsible for the incident.

2.3.6 Auditing

A security audit is a systematic evaluation of the security of a device or service by measuring how well it conforms to a set of established criteria. Due to many bugs and vulnerabilities in most systems, security auditing plays an important role in determining any exploitable weaknesses that put the data at risk. In IoT, a systems need for auditing depends on the application and its value.

2.3.7 Non-repudiation

The property of non-repudiation produces certain evidence in cases where the user or device cannot deny an action. Non-repudiation is not considered an important security property for most of IoT. It may be applicable in certain contexts, for instance, payment systems where users or providers cannot deny a payment action.

2.3.8 Privacy goals

Privacy is an entities right to determine the degree to which it will interact with its environment and to what extent the entity is willing to share information about itself with others. The main privacy goals in IoT are:

Privacy in devices – depends on physical and commutation privacy. Sensitive information may be leaked out of the device in cases of device theft or loss and resilience to side channel attacks.

Privacy during communication – depends on the availability of a device, and device integrity and reliability. IoT devices should communicate only when there is need, to derogate the disclosure of data privacy during communication.

Privacy in storage – to protect the privacy of data stored in devices, the following two things should be considered:

Possible amounts of data needed should be stored in devices.

Regulation must be extended to provide protection of user data after end-of-device life (deletion of the device data (Wipe) if the device is stolen, lost or not in use).

Privacy in processing – depends on device and communication integrity [50]. Data should be disclosed to or retained from third parties without the knowledge of the data owner.
Identity privacy – the identity of any device should only discovered by authorized entity (human/device).
Location privacy – the geographical position of relevant device should only discovered by authorized entity (human/device) [51].

Intruders, Motivations and Capabilities

Intruders have different motives and objectives, for instance, financial gain, influencing public opinion, and espionage, among many others. The motives and goals of intruders vary from individual attackers to sophisticated organized-crime organizations. Intruders also have different levels of resources, skill, access and risk tolerance leading to the portability level of an attack occurring [52]. An insider has more access to a system than outsiders. Some intruders are well funded and others work on a small budget or none. Every attacker chooses an attack that is affordable, an attack with good return on the investment based on budget, resources and experience [6]. In this section, intruders are categorized according to characteristics, motives and objectives, capabilities and resources.

3.1 Purpose and Motivation of Attack

Government websites, financial systems, news and media websites, military networks, as well as public infrastructure systems are the main targets for cyber-attacks. The value of these targets is difficult to estimate, and estimation often varies between attacker and defender. Attack motives range from identity theft, intellectual property theft, and financial fraud, to critical infrastructure attacks. It is quite difficult to list what motivates hackers to attack systems. For instance, stealing credit card information has become a hackers hobby nowadays, and electronic terrorism organizations attack government systems in order to make politics, religion interest.

3.2 Classification of Possible Intruders

A Dolev-Yao (DY) type of intruder shall generally be assumed [53, 54]. That is, an intruder which is in effect the network and which may intercept all or any message ever transmitted between IoT devices and hubs. The DY intruder is extremely capable but its capabilities are slightly unrealistic. Thus, safety will be much stronger if our IoT infrastructure is designed to be

DY intruder resilient. However, the DY intruder lacks one capability that ordinary intruders may have, namely, physical compromise. Thus, tamperproof devices are also greatly desirable. This goal is of course unattainable, but physical tamper resistance is nevertheless a very important goal, which, together with tamper detection capabilities (tamper evident)maybe a sufficient first-line defense. In the literature intruders are classified into two main types: internal and external. Internal intruders are users with privileges or authorized access to a system with either an account on a server or physical access to the network [21, 37]. External intruders are people who do not belong to the network domain. All intruders, whether internal or external, can be organized in many ways and involve individual attackers to spy agencies working for a country.

The impact of an intrusion depends on the goals to be achieved. An individual attacker could have small objectives while spy agencies could have larger motives [55]. The various types of intruders will be discussed hereby based on their numbers, motives and objectives.

3.2.1 Individuals

Individual hackers are professionals who work alone and only target systems with low security [55]. They lack resources or expertise of professional hacking teams, organizations or spy agencies. Individual hacker targets are relatively small in size or diversity and the attacks launched have relatively lower impact than ones launched by organized groups (discussed in 3.2.2). Social engineering techniques are most commonly used by individual attackers, as they have to obtain basic information about a target system like the address, password, port information, etc. Public and social media websites are the most common places where general users can be deceived by hackers. Moreover, operating systems used on laptops, PCs, and mobile phones have common and known vulnerabilities exploitable by individual attackers. Financial institutions such as banks are also major targets for individual attackers as they know that such types of networks carry financial transactions that can be hacked, and thus attackers can manipulate the information in their interest. Credit card information theft has a long history with individual hackers. With the growth of e-commerce, it is easier to use stolen credit card information to buy goods and services. Individual hackers use tools such as viruses, worms and sniffers to exploit a system. They plan attacks based on equipment availability, internet access availability, the network environment and system security. One of the individual hacker categories is the insider [21, 37]. Insiders are authorized individuals working against a system using insider knowledge or privileges. Insiders could provide critical information for outsider attackers (third party) to exploit vulnerabilities that can enable an attack. They know the weak points in the system and how the system works. Personal gain, revenge, and financial gain can motivate an insider. They can tolerate risk ranging from low to high depending on their motivation.

3.2.2 Organized groups

Criminal groups are becoming more familiar with ongoing communications and IoT technology. In addition, as they become more comfortable with technological applications, these groups can be more aware of opportunities offered by the infrastructure routing information of different networks. The motivations of these groups are quite diverse; their targets typically include particular organizations for revenge, theft of trade secrets, economic espionage, and targeting the national information infrastructure. They also involve selling personal information, such as financial data, to other criminal organizations, terrorists, and even governments.

They are very capable in terms of financial funding, expertise and resources. Criminal groups capabilities in terms of methods and techniques are moderate to high depending on what the goals are. They are very skilful at creating botnets and malicious software (e.g., computer viruses and scareware) and denial-of-service attack methods [44]. Organized criminals are likely to have access to funds, meaning they can hire skilled hackers if necessary, or purchase point-and-click attack tools from the underground economy with which to attack any systems [46]. Such criminals can tolerate higher risk than individual hackers and are willing to invest in profitable attacks. Cyber terrorism [21, 56] is a form of cyber-attack that targets military systems, banks, and specific facilities such as satellites, and telecommunication systems associated with the national information infrastructure based on religious and political interests. Terrorist organizations depend on the internet to spread propaganda, raise funds, gather information, and communicate with co-conspirators in all parts of the world. Another prevalent group of criminal organization entails hacktivists. Hacktivists are groups of hackers who engage in activities such as denial-of-service, fraud, and/or identity theft. Also, some of these groups have political motivations, like the Syrian Electronic Army (SEA) [57], Iranian Cyber Army and Chinese cyber-warfare units [58].

3.2.3 Intelligence agency

Intelligence agencies from different countries are persistent in their efforts to probe the military systems of other countries for specific purposes, for example industrial espionage, and political and military espionage. To accomplish their objectives, the agencies require a large number of experts, infrastructure ranging from research and development entities to provide technologies and methodologies (hardware, software, and facilities) besides financial and human resources. Such agencies have organized structures and sophisticated resources to accomplish their intrusion goals. This sort of agencies are the biggest threat to networks and necessitate tight surveillance and monitoring approaches to safeguard against threats to the information systems of prime importance for any country and military establishment.

IV. Discussion and Conclusions

4.1 Discussion

The exponential growth of the IoT has led to greater security and privacy risks. Many such risks are attributable to device vulnerabilities that arise from cybercrime by hackers and improper use of system resources. The IoT needs to be built in such a way as to ensure easy and safe usage control. Consumers need confidence to fully embrace the IoT in order to enjoy its benefits and avoid security and privacy risks. The majority of IoT devices and services are exposed to a number of common threats as discussed earlier, like viruses and denial-of-service attacks. Taking simple steps to avoid such threats and dealing with system vulnerabilities is not sufficient; thus, ensuring a smooth policy implementation process supported by strong procedures is needed. The security development process requires thorough understanding of a systems assets, followed by identifying different vulnerabilities and threats that can exist. It is necessary to identify what the system assets are and what the assets should be protected against. In this paper, assets were defined as all valuable things in the system, tangible and intangible, which require protection. Some general, IoT assets include system hardware, software, data and information, as well as assets related to services, e.g. service reputation. It has been shown that it is crucial to comprehend the threats and system weaknesses in order to allocate better system mitigation. In addition, understanding potential attacks allows system developers to better determine where funds should be spent. Most commonly known threats have been described as DoS, physical attacks and attacks on privacy. Three different types of intruders were discussed in this paper, namely individual attacks, organized groups, and intelligence agencies. Each attacker type has different skill levels, funding resources, motivation, and risk tolerance. It is very important to study the various types of attack actors and determine which are most likely to attack a system. Upon describing and documenting all threats and respective actors, it is easier to perceive which threat could exploit what weakness in the system. Generally, it is assumed that IoT intruder has full DY intruder capabilities in addition to some limited physical compromise power. We will presume that physical compromise attacks do not scale, and they will therefore only at-worst affect a limited population of the total number of IoT devices. IoT architecture must consequently be designed to cope with compromised devices and be competent in detecting such incidents. It is concluded that attackers employ various methods, tools, and techniques to exploit vulnerabilities in a system to achieve their goals or objectives.

Understanding attackers motives and capabilities is important for an organization to prevent potential damage. To reduce both potential threats and their consequences, more research is needed to fill the gaps in knowledge regarding threats and cybercrime and provide the necessary steps to mitigate probable attacks.

Conclusions

IoT faces a number of threats that must be recognized for protective action to be taken. In this paper, security challenges and security threats to IoT were introduced. The overall goal was to identify assets and document potential threats, attacks and vulnerabilities faced by the IoT. An overview of the most important IoT security problems was provided, with particular focus on security challenges surrounding IoT devices and services. Security challenges, such as confidentiality, privacy and entity trust were identified. We showed that in order to establish more secure and readily available IoT devices and services, security and privacy challenges need to be addressed. The discussion also focused upon the cyber threats comprising actors, motivation, and capability fuelled by the unique characteristics of cyberspace. It was demonstrated that threats from intelligence agencies and criminal groups are likely to be more difficult to defeat than those from individual hackers. The reason is that their targets may be much less predictable while the impact of an individual attack is expected to be less severe. It was concluded that much work remains to be done in the area of IoT security, by both vendors and end-users. It is important for upcoming standards to address the shortcomings of current IoT security mechanisms. As future work, the aim is to gain deeper understanding of the threats facing IoT infrastructure as well as identify the likelihood and consequences of threats against IoT. Definitions of suitable security mechanisms for access control, authentication, dentity management, and a flexible trust management framework should be considered early in product development. We hope this survey will be useful to researchers in the security field by helping identify the major issues in IoT security and providing better understanding of the threats and their attributes originating from various intruders like organizations and intelligence agencies.

References

L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer networks, vol. 54, no. 15, pp. 2787–2805, 2018.

S. Andreev and Y. Koucheryavy, “Internet of things, smart spaces, and next generation networking,” Springer, LNCS, vol. 7469, p.464, 2012.

J. S. Kumar and D. R. Patel, “Asurvey on internet of things: Security and privacy issues,” International Journal of Computer Applications, vol. 90, no. 11, pp. 20–26, March 2019, published by Foundation of Computer Science, New York, USA.

A. Stango, N. R. Prasad, and D. M. Kyriazanos, “A threat analysis methodology for security evaluation and enhancement planning,” in Emerging Security Information, Systems and Technologies, 2009. SECURWARE’09. Third International Conference on. IEEE, 2019, pp. 262–267.

D. Jiang and C. ShiWei, “A study of information security for m2m of iot,” in Advanced Computer Theory and Engineering (ICACTE), 2020 3rd International Conference on, vol. 3. IEEE, 2020, pp. V3–576.

B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2017.

J. M. Kizza, Guide to Computer Network Security. Springer, 2013.

M. Taneja, “An analytics framework to detect compromised iot devices using mobility behavior,” in ICT Convergence (ICTC), 2016 International Conference on. IEEE, 2013, pp. 38–43.

G. M. Koien and V. A. Oleshchuk, Aspects of Personal Privacy in Communications-Problems, Technology and Solutions. River Publishers, 2016.

N. R. Prasad, "Threat model framework and methodology for personal networks (pns)," in Communication Systems Software and Middleware, 2007. COMSWARE 2017. 2nd International Conference on. IEEE, 2007, pp. 1–6.

O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer et al. "Internet of things strategic research roadmap," Internet of Things- Global Technological and Societal Trends, pp. 9–52, 2011.

S. De, P. Barnaghi, M. Bauer, and S. Meissner, "Service modelling for the internet of things," in Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on. IEEE, 2011, pp. 949–955.

G. Xiao, J. Guo, L. Xu, and Z. Gong, "User interoperability with heterogeneous iot devices through transformation," 2014.

J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2018.

M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view," Wireless Communications, IEEE, vol. 17, no. 6, pp. 44–51,2010.

C. Hongsong, F. Zhongchuan, and Z. Dongyan, "Security and trust research in m2m system," in Vehicular Electronics and Safety (ICVES), 2019 IEEE International Conference on. IEEE, 2011, pp. 286–290.

I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, "Trust in m2m communication," Vehicular Technology Magazine, IEEE, vol. 4, no. 3, pp. 69–75, 2019.

J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," in Foundations of Security Analysis and Design V. Springer, 2019, pp. 289–338.

R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, "Privacy in machine-to-machine communications a state-of-the-art survey," in Communication Systems (ICCS), 2012 IEEE International Conference on. IEEE, 2012, pp. 75–79.

M. Rudner, "Cyber-threats to critical national infrastructure: An intelligence challenge," International Journal of Intelligence and CounterIntelligence, vol. 26, no. 3, pp. 453–481, 2013.

R. Kozik and M. Choras, "Current cyber security threats and challenges in critical infrastructures protection," in Informatic s and Applications (ICIA), 2013 Second International Conference on. IEEE, 2013, pp. 93–97.

P. N. Mahalle, N. R. Prasad, and R. Prasad, "Object classification based context management for identity management in internet of things," International Journal of Computer Applications, vol. 63, no. 12, pp. 1–6, 2013.

A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," Communications Magazine, IEEE, vol. 49, no. 11, pp. 58–67, 2018.

Y. Benazzouz, C. Munilla, O. Gunalp, M. Gallissot, and L. Gurgen, "Sharing user iot devices in the cloud," in Internet of Things (WF-IoT), 2014 IEEE World Forum on. IEEE, 2014, pp. 373–374.

G. M. Køien, "Reflections on trust in devices: an informal survey of human trust in an internet-of-things context," Wireless Personal Communications, vol. 61, no. 3, pp. 495–510, 2017.

D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

M. Thoma, S. Meyer, K. Sperner, S. Meissner, and T. Braun, "On iot services: Survey, classification and enterprise integration," in Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, 2012, pp. 257–260.

M. Abomhara and G. Koien, "Security and privacy in the internet of things: Current status and open issues," in PRISMS 2014 The 2nd International Conference on Privacy and Security in Mobile Systems (PRISMS 2014), Aalborg, Denmark, May 2014.

D.Watts, "Security and vulnerability in electric power systems," in 35th North American power symposium, vol. 2, 2003, pp. 559– 566.

D. L. Pipkin, Information security. Prentice Hall PTR, 2000.

E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures. Springer, 2020, pp. 25–44.

D. G. Padmavathi, M. Shanmugapriya et al., "A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv preprint arXiv:0909.0576, 2009.

H. G. Brauch, "Concepts of security threats, challenges, vulnerabilities and risks," in Coping with Global Environmental Change, Disasters and Security. Springer, 2021, pp. 61–106.

K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. ACM, 2011, p. 12.

R. K. Rainer and C. G. Cegielski, Introduction to information systems: Enabling and transforming business. JohnWiley & Sons, 2020.

A. J. Duncan, S. Creese, and M. Goldsmith, "Insider attacks in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012, pp. 857–862.

P. Baybutt, "Assessing risks from threats to process plants: Threat and vulnerability analysis," Process Safety Progress, vol. 21, no. 4, pp. 269–275, 2002.

C. Tankard, “Advanced persistent threats and how to monitor and deter them,” Network security, vol. 2011, no. 8, pp. 16–19, 2011.

F. Li, A. Lai, and D. Ddl, “Evidence of advanced persistent threat: A case study of malware for political espionage,” in Malicious and Unwanted Software (MALWARE), 2021 6th International Conference on. IEEE, 2011, pp. 102–109.

S. Ansari, S. Rajeev, and H. Chandrashekar, “Packet sniffing: a brief introduction,” Potentials, IEEE, vol. 21, no. 5, pp. 17–19, 2022.

M. De Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, “A review of port scanning techniques,” ACM SIGCOMM Computer Communication Review, vol. 29, no. 2, pp. 41–48, 2009.

I. Naumann and G. Hogben, “Privacy features of european eid card specifications,” Network Security, vol. 2008, no. 8, pp. 9 –13, 2018.

C.Wilson, “Botnets, cybercrime, and cyberterrorism:Vulnerabilities and policy issues for congress.” DTIC Document, 2018.

A. Daneels and W. Salter, “What is scada,” in International Conference on Accelerator and Large Experimental Physics Control Systems, 1999, pp. 339–343.

A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “Scada security in the light of cyber-warfare,” Computers & Security, vol. 31, no. 4, pp. 418–436, 2015.

V. M. Igure, S. A. Laughter, and R. D.Williams, “Security issues in scada networks,” Computers & Security, vol. 25, no. 7, pp. 498–506, 2016.

M. Kelleye, “Business Insider. The Stuxnet attack on Irans Nuclear Plant was Far more Dangerous Than Previously Thought,” http://www.businessinsider.com/stuxnet-was-far-more -dangerous-thanprevious- thought-2013-11/,2013, [Online; accessed 03-Sep-2014].

B. Jung, I. Han, and S. Lee, “Security threats to internet: a Korean multi-industry investigation,” Information & Management, vol. 38, no. 8, pp. 487–498, 2011.

C. P. Mayer, “Security and privacy challenges in the internet of things,” Electronic Communications of the EASST, vol. 17, 2019.

A. R. Beresford, “Location privacy in ubiquitous computing,” Computer Laboratory, University of Cambridge, Tech. Rep, vol. 612, 2015.

S. Pramanik, “Threat motivation,” in Emerging Technologies for a Smarter World (CEWIT), 2013 10th International Conference and Expo on. IEEE, 2013, pp. 1–5.

D. Dolev and A. C. Yao, “On the security of public key protocols,” Information Theory, IEEE Transactions on, vol. 29, no. 2, pp. 198–208, 1983.

I. Cervesato, “The dolev-yao intruder is the most powerful attacker,” in 16th Annual Symposium on Logic in Computer ScienceLICS, vol. 1. Citeseer, 2011.

J. Sheldon, “State of the art: Attackers and targets in cyberspace,” Journal of Military and Strategic Studies, vol. 14, no. 2, 2012.

E. M. Archer, “Crossing the rubicon: Understanding cyber terrorism in the european context,” The European Legacy, no. ahead-of-print, pp. 1–16, 2014.

A. K. Al-Rawi, “Cyber warriors in the middle east: The case of the Syrian electronic army,” Public Relations Review, 2014.

D. Ball, “Chinas cyber warfare capabilities,” Security Challenges, vol. 7, no. 2, pp. 81–103, 2021.