International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 4 ǁ April 2023 ǁ PP. 631-640

Cyber Security Trends: Its Implication and Ethical issues In the Philippines Setting

[1]Junie Q. Mansueto, [2]Atty. Stephen C. Olingay, [3]Kristine T. Soberano
[1] Northern Negros State College of Science and Technology, Old Sagay, Sagay City, Negros Occidental, Philippines
[2]College of Law-University of San Jose-Recoletos, Magallanes Street, Cebu City, Philippines
[3] Northern Negros State College of Science and Technology, Old Sagay, Sagay City, Negros Occidental, Philippines

Abstract
Devices connected to the Internet of Things (IoT) are quickly spreading throughout society, as are IoT services. Their success has not gone unnoticed, as seen by the rise in threats and assaults against IoT products and services. IoT cyberattacks are nothing new, but as IoT becomes more pervasive in our daily lives and communities, it becomes more important than ever to take cyber defense seriously. As a result, there is a genuine need to secure IoT, which has led to a requirement for a thorough understanding of vulnerabilities and attacks against IoT infrastructure. In addition to analyzing and characterizing attackers and intrusions against IoT devices and services, this article attempts to categorize different threat types.

Keywords: *Internet of Things, Cyber-attack, Security threats.*

Date of Submission: 11-04-2023 Date of acceptance: 26-04-2023

I. INTRODUCTION

Cybersecurity risks have escalated as a result of the Internet of Things (IoT) activities explosive growth, particularly for critical infrastructure. The world has seen an increase in cyber events over the past few years involving major industries like banking, water, power, and telecommunications which are essential to daily life and upholding societal functioning. These critical infrastructure disruptions are also quickly becoming a weapon for cyberwarfare against adversarial states. Therefore, protecting vital infrastructure from cyberattacks must be a top priority for any nation. The pandemic demonstrated how bad actors will seize any chance to undertake cyberattacks, especially during times of crisis when people are most helpless and exposed. Moving forward, it can be extremely beneficial to draw lessons from the collective experience of different nations in addressing the COVID-19 pandemic and the associated cybersecurity challenges. The level of cybersecurity in a nation can have a significant impact on that nation's foreign policy, economy, access to technology, and national security. To safeguard and maintain the provision of key services to people, cyber competence and readiness to recognize and respond to incidents are necessary. Foreign investment and citizen involvement in the global digital economy are influenced by cybersecurity policies and tactics. So that it can realize its full digital potential, nations should preserve and develop cybersecurity.

Threats are increasing daily, and attacks are becoming more frequent and sophisticated. The scale of networks and the pool of possible attackers are both expanding, and both are accompanied by an increase in the sophistication, efficacy, and effectiveness of the instruments at their disposal (Kizza, 2013; Schneier, 2011). IoT must therefore be protected from attacks and vulnerabilities to reach its full potential. Security is the process of preventing physical harm, illegal access, theft, or loss of an item by upholding the confidentiality and integrity of information about the object and making that information accessible whenever necessary (Kizza, 2013; Koien, 2013).

No object, tangible or not, can ever be in a secure condition and still be useful, hence according to Kizza (Kizza, 2013), there is no such thing as the secure state of any object. A procedure can preserve an object's greatest intrinsic value under a variety of circumstances. The IoT environment has the same security needs as any other ICT system. As a result, preserving the highest intrinsic value for tangible (devices) and intangible (services, information, and data) items is necessary to ensure IoT security.

With the use of numerous intrusions, including organizations and intelligence, this study aims to advance knowledge about threats and their characteristics (motive and capability). To establish a robust, comprehensive set of security criteria and to assess whether the security solution is secure against malicious assaults, it is required

to identify threats to systems and system weaknesses. Governments and IoT developers must finally comprehend the hazards and have the following information, in addition to users:

1. What are the assets?
2. Who are the principal entities?
3. What are the threats?
4. Who are the threat actors?
5. What capability and resource levels do threat actors have?
6. Which threats can affect what assets?
7. Is the current design protected against threats?
8. What security mechanisms could be used against threats?

The rest of this essay is structured as follows. The background, terminology, and main security and privacy objectives are provided in Section 2. In Section 3, many types of threat actors are outlined along with specific attacker motivations and capabilities. Section 4 serves as the paper's final section.

II. Background

The Internet of Things (IoT) (Andreev, 2012; Atzori, 2010) is an expansion of the Internet into the physical world enabling communication with nearby physical objects. As shown in Figure 1, the key concepts in the IoT area are entities, devices, and services. Between distinct projects, they have various definitions and meanings. Because of this, it's important to grasp what IoT entities, devices, and services are (in more depth in Section 2.1).

An IoT entity could be a person, an animal, a vehicle, a component of a supply chain, an electronic device, or a closed or open environment (Gubbi, 2013).

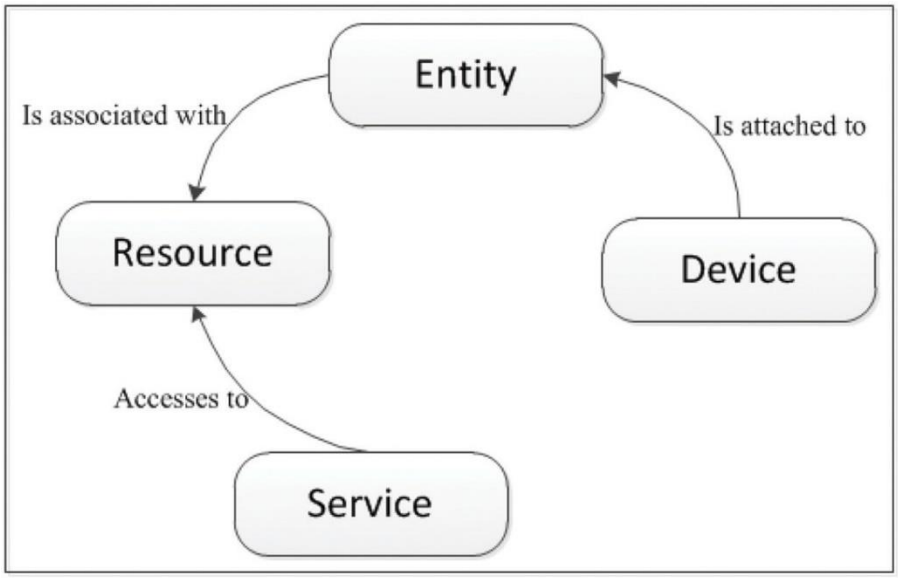

Figure 1 IoT model: key concepts and interactions.

Devices —hardware elements that enable entities to connect to the digital world—such as mobile phones, sensors, actuators, or RFID tags—make it feasible for entities to communicate with one another.

Machine-to-Machine (M2M) communication is the most widely used IoT application at the moment. To monitor and manage the user, machinery, and production processes in the global business, among other things, M2M is now widely used in the power, transportation, retail, public service management, health, water, oil, and other sectors (Cha, 2009; Du, 2010; Hongsong, 2011). By 2020, M2M applications are predicted to have 12 billion connections and provide 714 billion euros in revenue (Al-Rawi, 2014).

Along with all the advantages of IoT applications, several security risks have been noted (Cha, 2009; Roman, 2013). For various reasons, connected machines or devices are very desirable to cyber criminals.

1. Since most IoT devices are operated without human supervision, it is simple for an attacker to physically access them.
2. The majority of Internet of Things (IoT) components communicate over wireless networks, where an attacker might eavesdrop and collect private information.

3. Due to their low power and computing capacity, the majority of Internet of Things components cannot implement complicated security systems.

Furthermore, cyber threats could be launched against any IoT assets and facilities, threatening the general public, crippling system operations, or causing significant financial harm to owners and users (Cheng, 2012; Rudner, 2013). Attacks on home automation systems, as well as unauthorized access to lighting, heating, air conditioning, and physical security systems, are a few examples. The burglar may learn if someone is home or not from data gathered by sensors built into heating or lighting systems. Cyber-attacks could be launched, among other things, against any public infrastructure, such as utility systems (power systems or water treatment plants) (Kozik, 2013) to cut off the flow of electricity or water to residents.

With the move to the IoT, security, and privacy concerns are becoming more and more important to users and vendors (N.Mahalle, 2013). The extent of the harm brought about if any connected devices were compromised or hacked is undoubtedly simple to picture. It is widely acknowledged that integrating any IoT device into our personal, professional, or commercial surroundings might lead to new security issues. Users and vendors must take these security and privacy concerns into account and exercise caution.

2.1 Recognizing IoT Equipment and Services

The links between IoT components (IoT devices and IoT services) are detailed in this part, along with the key IoT domain concepts that are significant from the perspective of business processes.

2.1.1 IoT gadget

This piece of gear enables the creature to interact with the digital environment. It is also referred to as a "smart thing," which can be almost anything networked, equipped with actuators (such as light switches, displays, motor-assisted shutters, or any other action that a device is capable of performing), embedded computers, and sensors that provide information about the physical environment (e.g., temperature, humidity, presence detectors, and pollution).

IoT devices can communicate with each other as well as with ICT systems. These devices can communicate through several channels, such as wireless, cellular (3G or LTE), WLAN, or other technologies. The classification of IoT devices depends on their sizes, such as small or normal, mobility, such as mobile or fixed, external or internal power source, connectivity, automation, or non-automation, logical or physical objects, automated or non-automated, and finally, whether they are IP-enabled objects or non-IP objects.

IoT devices have actuation and/or sensing capabilities, the capacity to limit power and energy use, a connection to the physical world, sporadic connectivity, and mobility (N.Mahalle, 2013). While some might not, some must be quick, dependable, and give believable security and privacy (Koien, 2013). While some of these gadgets are physically guarded, others are left unattended.

Devices in IoT contexts need to be shielded from any dangers that could compromise their performance. However, because of their traits, the majority of IoT devices are susceptible to both internal and external threats (Hongsong, 2011). Due to limitations in IoT computing power, memory, and battery life, it is difficult to develop and use an effective security system.

2.1.2 Services Offered by IoT

IoT services make it simple for IoT devices to be integrated into the world of service-oriented architecture (SOA) and service science (Miorandi, 2012). A transaction involving the service provider and service user constitutes an IoT service, according to Thoma (Thoma, 2012). It causes a prescribed function, enabling contact with the physical world by assessing the state of entities or by initiating activities that will trigger a change in the entities.

Service offers a clear, standardized interface with all the features required for dealing with entities and related activities. By gaining access to a device's hosted resources, the services can reveal the functioning of the device.

2.1.3 Security in IoT Devices and Services

To ensure security, IoT devices, and services must be shielded from both internal and external illegal access. Services, physical resources, information, and data, both in transit and storage, should all be secured. Data confidentiality, privacy, and trust were the three main issues with IoT devices and services that we discussed in this section.

In IoT devices and services, data confidentiality poses a fundamental issue (Miorandi, 2012). In the IoT context not only the user may access data but also approved objects. Regarding the first, the access control and authorization mechanism, and the second, the authentication and identity management (IdM) mechanism, is necessary. The IoT device requires the ability to confirm that the entity (human or other devices) is permitted to access the service. Authorization helps determine if the person or device is permitted to receive a service upon

identification. Controlling access to resources involves utilizing a variety of criteria to allow or prohibit access. To connect various devices and services securely, authorization and access control are crucial. Making it simpler to establish, comprehend, and adjust access control rules is the major problem to be solved in this case. Authentication and identity management are other factors that should be taken into consideration when dealing with confidentiality.

The need for many individuals, objects/things, and devices to mutually authenticate through reliable services makes this problem crucial in the Internet of Things (IoT). The challenge is figuring out how to handle users, things/objects, and device identities securely. Due to the omnipresent nature of the IoT ecosystem, privacy is a crucial concern in IoT devices and services. Due to the interconnection of entities and the communication and exchange of data through the internet, user privacy is a touchy subject in many study efforts. There are still unresolved research questions regarding data security, data sharing, and privacy during data collection.

When many items connect in an unreliable IoT environment, trust is crucial to creating secure communication. According to Koien (Koien, 2013), the trustworthiness of an IoT device depends on the device components, including the hardware, such as processor, memory, sensors, and actuators, software resources, such as hardware-based software, operating system, drivers, and applications, and the power source. These two dimensions of trust should be taken into account in IoT: trust in the interactions between entities and trust in the system from the perspective of users (Abomhara, 2014). In a dynamic and collaborative IoT context, there should be a reliable process for defining trust to acquire the trust of users and services.

2.2 Security Attacks, Threats, and Vulnerabilities

The system assets (system components) that make up the IoT must first be recognized to address security concerns. Understanding the asset inventory, which includes all IoT components, devices, and services, is crucial. An asset is a financial resource, something priceless and delicate that belongs to an organization. Any IoT system's main assets are its system hardware (which may include structures, equipment, etc.), software, services, and data provided by the services.

2.2.1 Vulnerability

Vulnerabilities are flaws in a system's functionality or architecture that let an outsider run programs, gain access to private information, and/or launch denial-of-service attacks (Bertino, 2009). In IoT systems, vulnerabilities can be located in many different places. They may include but are not limited to, flaws in the system's hardware or software, in its policies and procedures, and in the system users themselves (Kizza, 2013). System hardware and system software, the two primary building blocks of IoT systems, frequently suffer design problems. Due to device compatibility and interoperability, as well as the effort required to address them, hardware vulnerabilities are exceedingly challenging to uncover and even more challenging to fix. Human deficiencies are typically the cause of technical vulnerabilities. A project starting without a plan, inadequate developer-to-user communication, a lack of resources, skills, and knowledge, as well as failure to manage and control the system are all effects of not understanding the requirements (Kizza, 2013).

2.2.2 Exposure

A flaw or error in the configuration of the system known as exposure makes it possible for an attacker to carry out information-gathering operations. Resilience against exposure to physical threats is one of the most difficult problems in IoT. Devices may be left unattended and placed in locations where they are likely to be easily accessible to attackers in the majority of IoT applications. Such exposure increases the likelihood that the device may be captured, its programming altered, or it could be replaced with a hostile device under the attacker's control.

2.2.3 Threats

An activity that exploits a system's security flaws and endangers it is considered a threat (Brauch, 2011). Humans and nature are the two main sources of threats (Dahbur, 2011). Natural disasters including hurricanes, floods, fires, and earthquakes could seriously harm computer systems. Natural disasters are difficult to protect against, and nobody can stop them from happening. The greatest methods for protecting systems from natural risks are disaster recovery plans, backup plans, and contingency plans. Human threats are those that are brought on by humans, such as malicious threats that are either external (someone operating outside the network) or inside (someone with allowed access) and aim to harm and disrupt a system. The following categories apply to hazards posed by people:

• Unstructured threats, made up primarily of novice users of readily accessible hacking tools.

• Structured threats because people are aware of system weaknesses and can comprehend, create, and use scripts and programs to their advantage. Advanced Persistent Threats (APT) are an illustration of a structured threat (Tankard, 2011). APT is a sophisticated network attack used to steal data from high-value information held by businesses and governments, including those engaged in manufacturing, finance, and national defense (Li, 2011).

The prevalence of IoT devices has increased security risks that could affect the broader public when IoT becomes a reality. IoT, however, introduces new security risks. There is a growing understanding that the new generation of smartphones, laptops, and other gadgets may be vulnerable to assault and targeted by malware.

2.2.4 Attacks

Attacks are acts taken to damage a system or obstruct regular operations by utilizing various strategies and tools to exploit vulnerabilities. Attackers launch attacks to accomplish objectives, either for their gratification or to receive retribution. The attack cost (Bertino, 2009) is a measurement of the effort that will be made by an attacker, represented in terms of their knowledge, resources, and motivation. Attack actors are those who pose a risk to the online environment (Schneier, 2011). Hackers, thieves, or even governments (Kizza, 2013) could be among them. Section 3 talks with more specifics.

An attack can take many different forms, such as close-range attacks, insider exploitation, active network attacks that monitor unencrypted traffic in search of sensitive information, passive attacks that watch unprotected network communications to decrypt weakly encrypted traffic, and so forth. Common forms of cyberattack include:
(a) Physical assaults: These assaults interfere with hardware elements. The majority of IoT devices often operate in outdoor settings, which are extremely vulnerable to physical attacks because of the unattended and scattered nature of the IoT.
(b) Reconnaissance attacks, which involve illegal system, service, or vulnerability detection and mapping. Scanning network ports (Ansari, 2002), using packet sniffers (De Vivo, 1999), traffic analysis, and sending requests for IP address information are a few examples of reconnaissance attacks.
(c) Denial-of-service (DoS): This type of attack aims to prevent the intended users from accessing a system or network resource. The bulk of IoT devices is susceptible to resource enervation attacks since they have minimal memory capacities and few computational resources.
(d) Access attacks: Unauthorized users access networks or devices they are not allowed to use. There are two sorts of access attacks: the first is physical access, in which the intrusive party gets access to a real object. The second is that IP-connected devices are subjected to remote access.
Attacks on privacy: Due to the vast amounts of information that are readily accessible through remote access mechanisms, privacy protection in IoT has grown to be more difficult. The most typical violations of user privacy include:
• Data mining: This technique enables attackers to find information in certain databases that was not expected.
• Cyber espionage: snooping on or obtaining confidential information from people, businesses, or the government using malicious software and cracking techniques.
• Eavesdropping: hearing what two parties are saying to one another (Naumann, 2008).
• Tracking: The device's unique identifying number (UID) allows for the tracking of a user's movements. When a user wants to remain anonymous, tracking their whereabouts makes it easier to identify them.
• Password-based attacks: intruders make an effort to mimic a legitimate user password. Two methods can be used to do this: 1) dictionary attack, which involves attempting various letter and number combinations to guess user passwords; and 2) Brute force attacks, in which cracking tools are used to test every possible combination of passwords to find working ones.
(f) Cybercrimes: The Internet and smart objects are used to commit crimes against people and their data, including fraud, grand theft, identity theft, and theft of intellectual property (Kizza, 2013; Schneier, 2011).
(g) Destructive attacks: Space is exploited to cause widespread disruption and property and human life loss. Terrorism and retaliation are two examples of damaging attacks.
(h) Attacks on Supervisory Control and Data Acquisition (SCADA) Systems: The SCADA system is susceptible to numerous cyberattacks (Igure, 2006; Nicholson, 2012)just like any other TCP/IP system. Any of the following methods of attack on the system is possible:
i. using denial-of-service to bring the system to a halt.
ii. gaining access to the system using Trojans or malware. For instance, a Stuxnet-based attack was conducted in 2008 against the Natanz nuclear complex in Iran (Kelley, 2013).

2.3 Main Security and Privacy Objectives

We need to be aware of the following major security objectives to develop effective IoT security:

2.3.1 Confidentiality

Although confidentiality is a crucial IoT security aspect, in other cases where data is made publicly available, it may not be required. However, sensitive information must generally not be shared with or read by unauthorized parties. Security credentials and secret keys, for instance, must be kept secret from unauthorized parties, as must medical data, information about private businesses, and/or information about the military.

2.3.2 Integrity

Integrity is typically a necessary security attribute to deliver trustworthy services to IoT users. The integrity requirements for various IoT systems vary (Jung, 2001). Due to information sensitivities, a remote patient monitoring system, for example, will include strong integrity checking against random errors. Communication mistakes or data manipulation could result in the loss of human life (Schneier, 2011).

2.3.3 Authentication and Authorization

Because of the nature of IoT environments—where it is feasible for communication to occur between M2M devices, humans, and/or humans—ubiquitous IoT connectivity exacerbates the authentication issue. Different systems need different solutions due to various authentication requirements. Some solutions, like the authentication of bank cards or banking systems, must be robust. On the other hand, while some will need to be local, such as ePassport, most will need to be international (Schneier, 2011). Only authorized entities (any authenticated entity) are permitted to carry out specific network actions thanks to the authorization attribute.

2.3.4 Availability

A device's user (or the device itself) must be able to access services whenever they are required. IoT devices' many hardware and software components must be durable to continue to function even in the presence of malevolent actors or challenging circumstances. various systems have various needs for availability. For instance, monitoring systems for fires or medical conditions would probably need more availability than sensors for roadside pollution.

2.3.5 Accountability

Accountability adds redundancy and responsibility for specific actions, obligations, and planning of the implementation of network security policies while building security solutions to be employed in a secure network. Although accountability by itself cannot thwart assaults, it is useful in verifying that the other security measures are effective.

2.3.6 Auditing

A security audit is a methodical assessment of a product's or service's security based on how well it complies with a set of predetermined standards. Security auditing is crucial in identifying any exploitable flaws that put the data at risk because the majority of systems have numerous bugs and vulnerabilities. A system's need for auditing in the Internet of Things depends on its use and value.

2.3.7 Non-repudiation

In circumstances where the user or device is unable to refute an activity, the property of non-repudiation yields specific proof. For the majority of IoT, non-repudiation is not seen as a crucial security attribute. It might be appropriate in some situations, such as payment systems when consumers or suppliers are unable to refuse a payment action.

2.3.8 Privacy goals

Privacy is the right of an entity to choose how much it will interact with its environment and how much of its personal information it will share with others. IoT's primary privacy objectives are:

• Device privacy is dependent on physical and commuter privacy. When a device is stolen or lost, or if it is vulnerable to side-channel assaults, sensitive information may leak out of it.

• Communication privacy is dependent on device availability, device integrity, and device dependability. IoT devices should only communicate when necessary to prevent the leaking of private data while communicating.

• Storage privacy - The following two factors should be taken into account to safeguard the privacy of data stored on devices:

  • Devices should be prepared to store any necessary data amounts.

  • Regulation must be expanded to enable user data protection after the end of a device's useful life (deletion of the device data, or "Wipe," if lost, stolen, or not in use).

• Processing privacy is device and communication integrity dependent. Without the data owner's knowledge, data should be released to or obtained from third parties.

• identify privacy - Only authorized entities (humans or devices) should be able to determine the identity of any device.

• Location privacy - Only authorized entities (humans or devices) should be able to determine the precise location of the relevant device.

III. Intruders, Motivations, and Capabilities

Intruders are motivated by a variety of reasons, including espionage, monetary gain, and public opinion manipulation, among many others. Individual attackers and sophisticated organized crime organizations have different motivations and objectives when breaking in. The mobility of an assault is influenced by the resources, expertise, access, and risk tolerance of the intruders (Pramanik). A system is more accessible to insiders than to outsiders. Some invaders have substantial funding, while others have little to no funding. Based on their budget, resources, and experience, every attacker selects an approach that will yield a favorable return on investment (Schneier, 2011). Intruders are classed in this section based on traits, motivations and objectives, capabilities, and resources.

3.1 Purpose and Motivation of Attack

The main targets of cyberattacks are public infrastructure systems, banking systems, news and media websites, military networks, and government websites. It is challenging to determine the worth of these targets, and attackers and defenders frequently have different estimates.

3.2 Classification of Possible Intruders

It is widely considered that an intruder is of the Dolev-Yao (DY) type (Dolev, 1983). That is a hacker who is on the network and can intercept any message ever sent between IoT hubs and devices. The DY invader is quite powerful, although some of its skills are slightly exaggerated. Therefore, if our IoT system is created to be DY intruder-resilient, safety will be considerably greater. The DY intruder lacks physical compromise, a skill that common intruders might possess. Therefore, tamper-proof technology is also highly desired. Although this objective is unachievable, physical tamper resistance is nevertheless a crucial goal that, when combined with tamper detection abilities (tamper evident), may be an adequate first line of protection. The two basic categories of intruders in the literature are internal and external. Users having access privileges or authorization to a system who have physical access to the network or a server account are considered internal invaders (Duncan, 2012; Rudner, 2013). People who do not belong to the network domain are considered external intruders. All invaders, whether internal or foreign, can be arranged in a variety of ways, from lone assailants to national surveillance agencies. The consequences of an intrusion depend on the objectives that must be met. An individual attacker may have limited goals, whereas a spy agency may have more significant ones. Based on their numbers, motivations, and goals, the many categories of intruders will be examined in this article.

3.2.1 Individuals

Individual hackers are experts who primarily target systems with inadequate security and work alone. They don't have the resources or know-how that professional hacking teams, organizations, or spies do. Attacks launched by individual hackers tend to be less effective than those launched by organized groups since their targets are typically smaller or less diverse (described in 3.2.2). Since they need to learn the address, password, port information, and other essential details about a target system, individual attackers are most likely to use social engineering techniques. The most popular websites where regular users might be tricked by hackers are public and social media platforms. Additionally, mobile phone, PC, and laptop operating systems all have widespread, well-known flaws that can be utilized by lone attackers. The insider is one of the distinct sorts of hackers (Duncan, 2012; Rudner, 2013). Insiders are authorized people who use insider information or access to the system to fight against it. Insiders might give outside attackers (third parties) vital knowledge they need to find and exploit vulnerabilities and launch an attack. They are familiar with the system's workings and weak spots. An insider may be motivated by personal benefit, retaliation, or financial gain. Depending on their motive, they can bear risks ranging from low to high.

3.2.2 Organized groups

The Internet of Things (IoT) and continuing communications are becoming more known to criminal organizations. Additionally, as these organizations gain experience with technological applications, they may become more conscious of the opportunities provided by the infrastructure routing data of various networks. These organizations frequently serve as their targets for vengeance, theft of trade secrets, economic espionage, and attacks on the national information infrastructure. The reasons for these groups are fairly varied. They also involve selling private data, including financial information, to terrorists, governments, and other criminal organizations. They have a lot of resources, knowledge, and financial backing. Depending on their objectives, criminal organizations have modest to high capabilities in terms of strategies and procedures. They have a great deal of expertise in the development of botnets, harmful software (such as computer viruses and scareware), and denial-of-service attack techniques. Organized criminals are likely to have access to money, which enables them to attack any system by themselves or, if necessary, by hiring professional hackers from the black market (Nicholson, 2012). These criminals are ready to invest in successful attacks and can tolerate greater risk than individual

hackers. According to religious and political motives, cyberterrorism (Archer, 2014; Rudner, 2013) is a type of cyber-attack that targets military systems, banks, and specific locations like satellites and telecommunication networks that are part of the national information infrastructure.

Using the internet, terrorist groups can disseminate propaganda, generate money, acquire intelligence, and interact with associates around the globe. Hacktivists are another common type of criminal organization. Groups of hackers known as hacktivists participate in illegal acts such as denial-of-service attacks, fraud, and/or identity theft. Additionally, some of these organizations—such as the Syrian Electronic Army (SEA) (Al-Rawi, 2014), the Iranian Cyber Army, and Chinese cyberwarfare forces—have political objectives.

3.2.3 Intelligence agency

To conduct certain types of espionage, such as industrial espionage and political and military espionage, intelligence agencies from various nations are steadfast in their efforts to examine the military systems of other nations. The agencies need a lot of expertise, and infrastructure from research and development organizations to supply technologies and methodologies (hardware, software, and facilities), together with financial and human resources, to achieve their goals. Such organizations use well-organized systems and cutting-edge tools to achieve their intrusive objectives. These organizations pose the greatest risk to networks, necessitating stringent surveillance and monitoring measures to prevent threats to the crucial information systems for every nation and military installation.

IV. RESULT AND DISCUSSION

IoT security and privacy threats have increased as a result of the IoT's exponential expansion. Many of these threats are caused by hardware flaws brought on by hacker cybercrime and inappropriate system resource usage. The IoT must be designed in a way that makes easy and secure usage control possible. For consumers to fully benefit from the IoT and avoid security and privacy threats, they must have the confidence to do so.

As was previously said, the majority of IoT devices and services are vulnerable to several typical threats, including viruses and denial-of-service assaults. Simple precautions won't be enough to protect against such dangers and address system weaknesses; instead, it's important to ensure that policies are implemented smoothly and are supported by reliable procedures. A detailed understanding of a system's assets is necessary for the security development process, which is followed by the identification of potential threats and vulnerabilities. It is important to define the system assets and the threats they should be safeguarded from. Assets were outlined in this study as all valuable items in the system, both tangible and intangible, that need to be safeguarded. IoT assets in general include things like system hardware, software, data, and information, as well as things like service-related assets like service reputation. It has been demonstrated that to allocate effective system mitigation resources, it is essential to understand the risks and system weaknesses. Additionally, being aware of prospective assaults helps system developers decide where money should be allocated more wisely. The most well-known threats have been categorized as DoS, physical attacks, and privacy attacks.

In this research, three basic sorts of intruders—individual attacks, organized organizations, and intelligence agencies—were covered. Each sort of attacker has a varied risk tolerance, financial resources, skill set, and motive. It is crucial to research the different categories of attack actors and identify those that are most likely to target a system. It is simpler to understand which danger could take advantage of which system vulnerability after all threats and their associated actors have been described and documented. Generally speaking, it is thought that IoT intruders have limited physical compromise power in addition to full DY intrusion capability. Assuming physical compromise attempts do not scale, they will, at worst, only have a minor impact on the overall population of IoT devices. It is established that to accomplish their goals or objectives, attackers use a variety of tools, methods, and strategies to exploit vulnerabilities in a system. An organization must comprehend the intentions and capabilities of potential attackers to limit any harm. More research is required to close the knowledge gaps about risks and cybercrime, offer the essential actions to minimize likely attacks and reduce both prospective threats and their effects.

V. CONCLUSION

IoT faces a variety of risks, all of which must be understood to take appropriate precautions. The problems and dangers of IoT security were discussed in this article. The main objective was to list assets and record potential threats, assaults, and weaknesses the IoT may encounter. With an emphasis on security issues involving IoT devices and services, a summary of the most significant IoT security issues was presented. Confidentiality, privacy, and entity trust were recognized as security challenges. We demonstrated that security and privacy issues must be resolved to create IoT devices and services that are safer and easily accessible. The

debate also centered on cyber threats, which included people, motives, and capabilities fueled by the particularities of cyberspace. Threats posed by criminal organizations and intelligence services were shown to be more challenging to counter than those posed by lone hackers. The reason for this is that, while the effects of a single strike are anticipated to be less severe, their targets may be considerably less predictable. It was determined that both providers and end users still have a lot of work to do in the area of IoT security. Future standards must address the inadequacies of the IoT security systems in use today. Future studies will focus on developing a greater knowledge of the dangers to IoT infrastructure as well as determining their likelihood and potential effects. Early in the product development process, adequate security definitions for access control, authentication, identity management, and a flexible trust management framework should be taken into account. By assisting in the identification of the key problems with IoT security and offering a better understanding of the risks and their characteristics originating from different intruders like organizations and intelligence agencies, we believe that this survey will be helpful to researchers in the security sector.

REFERENCES

[1]. Abomhara, M., & Koien, G. M. (2014). Security and privacy in the Internet of things: Current status and open issues. 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS).

[2]. Al-Rawi, A. K. (2014). Cyber warriors in the Middle East: The case of the Syrian Electronic army. Public Relations Review, 40(3), 420-428.

[3]. Andreev, S., Balandin, S., & Koucheryavy, Y. (2012). Internet of things, smart spaces, and next-generation networking: 12th International Conference, NEW2AN 2012, and 5th conference, ruSMART 2012, St. Petersburg, Russia, August 27-29, 2012, proceedings. Springer.

[4]. Ansari, S., Rajeev, S., & Chandrashekar, H. (2002). Packet sniffing: A brief introduction. IEEE Potentials, 21(5), 17-19.

[5]. Archer, E. M. (2014). Crossing the Rubicon: Understanding cyber terrorism in the European context. The European Legacy, 19(5), 606-621.

[6]. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.

[7]. Bertino, E., Martino, L. D., Paci, F., & Squicciarini, A. C. (2009). Web services threats, vulnerabilities, and countermeasures. Security for Web Services and Service-Oriented Architectures, 25-44.

[8]. Brauch, H. G. (2011). Concepts of security threats, challenges, vulnerabilities, and risks. Hexagon Series on Human and Environmental Security and Peace, 61-106.

[9]. Cha, I., Shah, Y., Schmidt, A., Leicher, A., & Meyerstein, M. (2009). Trust in M2M communication. IEEE Vehicular Technology Magazine, 4(3), 69-75.

[10]. Cheng, Y., Naslund, M., Selander, G., & Fogelstrom, E. (2012). Privacy in machine-to-machine communications a state-of-the-art survey. 2012 IEEE International Conference on Communication Systems (ICCS).

[11]. Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011). A survey of risks, threats, and vulnerabilities in cloud computing. Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications.

[12]. De Vivo, M., Carrasco, E., Isern, G., & De Vivo, G. O. (1999). A review of port scanning techniques. ACM SIGCOMM Computer Communication Review, 29(2), 41-48.

[13]. Dolev, D., & Yao, A. (1983). On the security of public key protocols. IEEE Transactions on Information Theory, 29(2), 198-208.

[14]. Du, J., & Chao, S. (2010). A study of information security for M2M of IOT. 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE).

[15]. Duncan, A. J., Creese, S., & Goldsmith, M. (2012). Insider attacks in cloud computing. 2012 IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communications.

[16]. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[17]. Hongsong, C., Zhongchuan, F., & Dongyan, Z. (2011). Security and trust research in M2M system. Proceedings of 2011 IEEE International Conference on Vehicular Electronics and Safety.

[18]. Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498-506.

[19]. Jung, B., Han, I., & Lee, S. (2001). Security threats to the internet: A Korean multi-industry investigation. Information & Management, 38(8), 487-498.

[20]. Kelley, M. B. (2013, November 20). The Stuxnet attack on Iran's nuclear plant was 'Far more dangerous' than previously thought. Business Insider.

[21]. Kizza, J. M. (2013). Guide to computer network security. Springer Science & Business Media.

[22]. Koien, G. M., & Oleshchuk, V. A. (2013). Aspects of personal privacy in communications: Problems, technology, and solutions. River Publishers.

[23]. Kozik, R., & Choras, M. (2013). Current cyber security threats and challenges in critical infrastructures protection. 2013 Second International Conference on Informatics & Applications (ICIA).

[24]. Li, F., Lai, A., & Ddl, D. (2011). Evidence of advanced persistent threat: A case study of malware for political espionage. 2011 6th International Conference on Malicious and Unwanted Software.

[25]. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516.

[26]. N.Mahalle, P., Rashmi Prasad, N., & Prasad, R. (2013). Object classification-based context management for identity management in the Internet of Things. International Journal of Computer Applications, 63(12), 1-6.

[27]. Naumann, I., & Hogben, G. (2008). Privacy features of European Eid card specifications. Network Security, 2008(8), 9-13.

[28]. Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. Computers & Security, 31(4), 418-436.

[29]. Pramanik, S. (2013). Threat motivation. 2013 10th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT).

[30]. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of things. Computer Networks, 57(10), 2266-2279.
[31]. Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and Counterintelligence, 26(3), 453-481.
[32]. Schneier, B. (2011). Secrets and lies: Digital security in a networked world. John Wiley & Sons.
[33]. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network Security, 2011(8), 16-19.
[34]. Thoma, M., Meyer, S., Sperner, K., Meissner, S., & Braun, T. (2012). On IoT-services: Survey, classification, and enterprise integration. 2012 IEEE International Conference on Green Computing and Communications.