International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Review : Cyber Crime

Dinker Kumar[1], **Vinod Mahor**[2]

[1]M Tech Scholar, Department of Computer Science & Engineering, Millennium Institute of Technology & Science Bhopal, India

[2]Assistant Professor, Dept. of Computer Science & Engineering, Millennium Institute of Technology & Science Bhopal, India

ARTICLEINFO

Article History:

Accepted: 10 April 2023
Published: 30 April 2023

Publication Issue
Volume 9, Issue 2
March-April-2023

Page Number
693-705

ABSTRACT

Devices connected to the Internet of Things (IoT) are evolving to become increasingly universal. In the current climate, it is impossible to deny the success of the Internet of Things (IoT). Concurrently, assaults and threats against IoT devices and facilities are also rising on a daily basis. It is imperative that efforts be made to safeguard cyberspace seriously since cyberattacks are increasingly becoming ingrained in the Internet of Things (IoT) and damaging users' lives as well as society. The infrastructure of governments and enterprises throughout the world is at risk from cybercrimes, which may also cause consumers harm in a variety of different ways. With the losses caused by global cybercrime expected to cost up to 6 trillion dollars yearly on the worldwide economy by cybercrime, it is clear that this problem has to be addressed immediately. It is estimated that Australia suffers annual damages up to 328 million dollars as a result of cyberattacks. There are a number of measures tried to slow down these assaults, but sadly they are unable to accomplish results to the desired degree. As a result, making the Internet of Things (IoT) safe is an absolute necessity in the modern world, and the structure of IoT should be thoroughly investigated. There are several potential causes for cyberattacks, including: 1. nations with inadequate cyber security; 2.2. Cybercriminals launch their attacks using cutting-edge technology. 3. Services and other business plans can be used to engage in criminal activity in cyberspace. When it comes to the battle against cybercrime, Managed Service Providers (MSP) have a unique set of challenges. They are responsible for ensuring not just the safety of that particular customer, but also the safety of all of their servers, devices, and other systems. Therefore, they are required to utilize antivirus and anti-malware products that are efficient, quick, and simple to operate.

Keywords: Cyber-crimes, cyber-attacks, IoT, IoT Ap- plications, Smart Cities

I. INTRODUCTION

The Internet of things (IoT) is expanding at a breakneck pace, and because it provides many different kinds of services, it has become the most quickly expanding technology that has a significant impact on the infrastructures of both society and businesses. The Internet of Things (IoT) has become an essential component of contemporary human existence, appearing in spheres as diverse as education, every kind of business, healthcare, and the storage of confidential data pertaining to corporations and individuals, as well as details regarding financial transactions, the creation of a product, and its promotion [37, 49]. When it comes to the Internet of Things (IoT), transmission from linked devices has caused a great need to concentrate on security. This is due to the fact that millions and billions of people conduct sensitive transactions online. The sophistication and frequency of assaults and dangers in cyberspace are growing constantly.

as well as numbers. The expansion of networks has resulted in an increase in the number of potential attackers, and the tools and tactics that these attackers employ are likewise growing more effective, efficient, and complex [15]. As a result, in order to get the most of the Internet of Things' capabilities, it is necessary to safeguard it against dangers and assaults. The security of smart devices or technologies such as hot spots, the internet, and other internet of things (IoT) has been compromised since they have become integrated into every aspect of human existence [20].

These intelligent technologies do, in fact, have a lot of benefits to provide; but, they also have a lot of flaws, which results in the risk of cyberattacks that will inflict a significant amount of harm to both life and property. To eliminate the risk of being hacked or scammed in the current environment, it is necessary to implement technologies that come equipped with adequate security measures across the board. 98% of all the traffic coming from IoT devices is not encrypted, which leaves personal and private information exposed on the network [27]. IP-Phones, which account for 44% of corporate IoT Devices but only 5% of security concerns when compared to other IoT devices, are the Internet of Things device that is utilized the most in businesses and on a daily basis in the workplace. The majority of security problems are caused by cameras, which provide 33% of a danger yet are only used 5% of the time in commercial settings [21], [22].

According to the statistics from the Australia cybersecurity centre, there has been one recorded incident every 10 minutes, which results in yearly losses of $328 million for Australian economy. Identity theft, online fraud, and shopping scams, bulk extortion, online romance scams, wire-fraud, and business email compromise are the top five forms of cybercrime that target Australians [26]. Other types include wire-fraud, business email compromise, and online romance scams. According to statistics collected by Agari, between December 2019 and June 2020, 68% of identity-deception-based assaults targeted at impersonating a trusted people or brand. According to data from Kaspersky, an estimated 105 million assaults on Internet of Things devices are originating from 276,000 distinct IP addresses. As a proxy service, cybercriminals utilize networks to infect smart devices, which they then employ to launch DDoS assaults. Imaging equipment account for 51% of all health care devices that are targeted by cybercriminals [53]. Peer-to-peer command and worm-like capabilities for self-propagation are two examples of the new tactics that are being used to infect susceptible Internet of Things devices on the same network [50].

II. LITERATURE REVIEW

The authors Yang Lu and Li Da Xu (2019) analyze the idea that the Internet of Things (IoT) has modernized the network on a global scale, integrating intelligent equipment, people, other intelligent items, and information. The Internet of Things offers a chance to improve integrity, confidentiality, accessibility, and availability of information. The internet of things is still in the process of being developed, and as such, it has a great deal of unresolved problems that need to be addressed [1]. IoT growth must begin with a solid foundation in system security. The topic of cybersecurity is investigated in great detail in this paper. In the realm of information and communication, the primary focus is on the safeguarding and integration of a wide variety of intelligent devices and technology. This study makes it possible for other academics and industry professionals who are interested in doing research on the Internet of Things in the future to obtain knowledge that is helpful [39]. The report demonstrates research on cybersecurity for the internet of things, as well as taxonomy and architecture for internet of things cybersecurity, as well as other research trends and difficulties.

S. Hilt; V. Kropotov; F. Merces; and M. Rosario are the authors of the study. in addition to Sancho, D. (2017) conclude that the Internet of Things is having an effect on every sector of contemporary civilization. The ever-increasing development of IoT presents a new challenge for cybersecurity experts [2]. A variety of Studies are being conducted to determine how criminals might target the internet of things and what kind of an impact this will have. For the purpose of this study, the IoT cyber-crime underworld was chosen to solicit thoughts on contemporary concerns from a variety of minds that contemplate them. It is determined that there are five subterranean organizations, and these groups are classified according to the terminology that is utilized in community discussions, i.e. Multiple languages, including English, Spanish, Portuguese, and Russian. There is a large amount of research and tutorials that have been accumulated on the way of hacking, the exploitation of vulnerability; yet, there is no sign of any intensive determination from the criminal's clusters to cause massive damage to IoT structures. The pursuit of financial gain is often what motivates cybercriminals, but there are currently very few methods to benefit from attacks on the internet of things (IoT). Cybercriminals are always coming up with new tools that allow them to find new methods to infect computers and generate a lot of money off of the viruses they spread.

Drs. A. Venckauskas, R. Damasevicius, V. Jusas, J. Told-inas, and D. Rudzika were the researchers that conducted the study. as well as Dregvaite, G. (2015) came to the conclusion that the Internet of Things may be conceptualized as a physical network that is a part of the world wide web and that connects all different kinds of physical objects that are present on the internet. There are a lot of moving parts in the Internet of things [3]. Because of its massive scale, expansive breadth, and widespread physical distribution, the Internet of Things (IoT) is notoriously difficult to defend against the dangers posed by cybercriminals [38]. The Internet of Things has several limitations, such as limited power, which contribute to the difficulties by prohibiting the use of high-security but resource-hungry cryptography [23]. This is one of the ways that the limitations contribute to the problems. The Internet of Things (IoT) creates the conditions for cybercrime. In order to trick users of Internet of Things technology and security measures, hackers and other malicious actors capitalize on the fact that consumers have a limited understanding of these topics. There is a growing need for innovative approaches to digital forensics in the Internet of Things (IoT), as the number of potential dangers and assaults, both current and foreseeable, continues to rise. The field of digital forensics is always facing new problems as a result of the ongoing development of new technology and new tactics. The Internet of Things stores a significant quantity of data. Huge scope, a big volume of data, different nature of the Internet of things, and ways in which information is shared, combined, and handled need the development of new tactics by the digital forensic investigations. This is because the methods in which information is shared, combined, and handled are constantly evolving. It has been discovered that the old forensic procedures that are employed in the investigation of cybercrimes are completely ineffective, since cybercriminals are constantly developing new tools and gadgets to con users who utilize the internet of things (IoT) [32].

The author is M. Abomhara. in addition to Koien, G. M. (2015) discovered that there is still a significant amount of work to be done in the subject of Internet of Things (IoT) security by merchants and end-users. Because the internet of things is expanding at such a rapid rate, it is essential to investigate potential threats to its security. Threats and assaults on the infrastructure of the internet of things should be extensively studied, along with the effects of these threats and attacks on the internet of things [4]. It is strongly recommended that effective security devices for regulating access, authenticating users, managing identities, and providing a flexible structure for trust management be included right from the beginning of the product development process. This research is helpful for academics who study the topic of security because it assists in locating the primary problems with the insecurity of IoT and provides a clear grasp of threats and assaults as well as the variables that are instigated by a variety of companies or intelligence agencies. This research contributes to improve clarity on numerous risks and the variables that contribute to them, including intelligence and organizations among other types of potential intruders [28]. To maintain a healthy and secure environment, it is essential to go through the process of identifying potential dangers and openings. provide a fully protected and secure IoT environment, as well as check that the security solution is robust enough to withstand hostile assaults.

J. Iqbal, along with B. M. Beigh (2017) investigates the idea that as the number of people using the internet grows across the world, the number of people committing crimes online likewise grows at the same rate, notably in India[5]. In the same way that cybercrime is not limited to a particular region of the world, the Internet of Things (IoT) spans huge territories all over the planet. Therefore, the local laws simply cannot be used to manage these offenses. In the context of India, cyber laws are still in the beginning stages of the development process. As part of its efforts to modernize its cyber space, India has entered into a number of bilateral agreements concerning cyber-crime, such as the deal with Russia, a fundamental agreement with the United States, and a framework cyber pact with Israel. However, the breadth of these bilateral agreements is restricted, rendering them useless and inadequate for combating cybercrime. According to the findings of this study, India ought to establish a multilateral treaty that blends its laws on common criminal policy and makes a deal to minimize instances of cybercrime on a worldwide level through cooperation with international organizations. This convention will aid in the drafting of active rules and powerful analytical methodologies, which will result in an increase in globally cooperative efforts to combat cyber-crime [45]. One of the multilateral international treaties that deal with international cooperation for the purpose of combating cybercrime throughout the world is known as the Budapest treaty council of Europe on cybercrime. Since the United States and Israel, with which India already has bilateral agreements, are already parties to the Budapest Convention on Cybercrime, India too need to become a member of this convention.

A. Sarmah and R. Sarmah. Sarmah. in addition to Baruah, A. J. (2017) discovered that as a result of the development of new technologies, there was also an increase in the number of crimes connected to the Internet of Things [6]. Because cybercrime is a genuine danger to people, it is essential to take precautions to safeguard the internet of things (IoT) from cybercriminals for the sake of the welfare of society, cultural preservation, and the security of countries.

The Information Technology Act of 2000 was passed by the Indian government in an effort to manage concerns relating to cybercrime. The commission of cybercrime is not restricted to any one geographical place in particular. It is tough to investigate and bring criminals to justice since it transcends national boundaries on the internet and presents legal and technical obstacles. As a result, it is imperative that appropriate measures be made to exercise control over cybercrimes on a global scale. In order to effectively combat cybercrime, governments from all around the world must work together in close collaboration and coordination. The dissemination of information on cybercrime to members of the general public is the primary purpose of this research. It is essential for users who have been the victim of cybercrime to come forward and submit a report against the perpetrators of the crime. This will allow for stern steps to be taken against the perpetrators, as well as serve as an example for users who commit cybercrime in the future.

MS. Anisha (2017) contends that technology and the risky architecture of the Internet of Things (IoT) are the primary contributors to the rise of cybercrime. The rise in the number of people using Internet of Things platforms brings with it an increase in the likelihood of a variety of cybercrimes. The introduction of new technology has led to an unforeseen increase in criminal activity. The number of crimes committed using various forms of technology continues to rise, making it imperative that these cases be resolved as quickly as possible [7]. Crimes committed online are not restricted to just taking place on computers; they may also involve other electronic devices, such as those used for communications or financial transactions, and so on. Because of the varied nature of IoT, it can be challenging to identify potential vulnerabilities in terms of cyber security, which might lead to ignorance regarding various security concerns. To raise people's levels of consciousness, it has been recommended that free seminars and commercials be arranged. among users with the assistance of non-governmental organizations and the government. Issues and concerns related to cybercrime should be addressed at the grassroots level, which includes institutions, schools, universities, and other computer centers, among other places. The Indian government has adopted a number of measures that have shown to be beneficial in the fight against cybercrime, such as passing the Information Technology Act, 2000. However, a static cyber law is ineffective in the context of cyber-crime due to the nature of IoT, which is large and diverse, as well as the fact that new types of crimes are constantly being invented. Therefore, it is essential for the field of cyber law to maintain a careful eye on the rise of cybercrime and keep its laws and regulations up to date accordingly.

M. Hesamuddin and M. Qayyum respectively. 2017 is the year that you should investigate how the internet of things is becoming into an important technology. The data that can be conveyed via RFID tags or sensors includes sensitive information that ought to be protected from access by unauthorized parties. There is no security in the communication that takes place between two nodes of the internet of things, and the security of the internet of things should not be bargained [8]. It is required for the Internet of Things to have services such as end-to-end environments, real-time access control, security of vital infrastructure, and encryption in order to achieve the goal of achieving more secure communication. It is impossible to think like a cybercriminal or to keep one step ahead of them. It is reasonable to anticipate that in the not-too-distant future, smart devices will have privacy security features that will enable users to carry out more chores more simply with the aid of IOT. In this increasingly connected world, the Internet of Things (IoT) will earn the confidence and faith of consumers if it can improve its privacy protections, methodologies, and ethical practices.

North-East of Marion. (2010) contends that the Agreement on Cybercrime established by the Council of Europe (CoE) should be investigated as a representative instrument. This research demonstrates that the Agreement contains the characteristics of a metaphorical policy, such as assuring users that appropriate action is being taken to regulate cybercrime, educating users about cybercrime, and serving as a warning for those who conduct cybercrimes. It has major repercussions for the Internet of Things [9]. Since crimes committed using computers are worldwide in nature, they are not limited to the jurisdiction of any one particular nation. It is important for nations to work together and align their legal systems in order to effectively combat cybercrime. The Coe pact is a very significant step towards the regulation and prevention of cybercrime on a worldwide scale. Because the scope of cybercrime is so expansive, it is extremely challenging to exercise adequate control over it. In the process of developing this treaty, officials from many nations discuss and debate the acts that have been perpetrated via the internet and describe the steps that may be taken to combat cyber-crimes [33]. For the purpose of controlling cybercrimes, a dependable worldwide strategy is utilized, which entails cooperation between law enforcement agencies and the investigation of offenses. The discovery demonstrates that the efficacy of the CEO Treaty is problematic due to the fact that the resolutions stated in this treaty are essentially metaphorical. These resolutions include concerns pertaining to privacy, the powers of investigators, and the fact that it is rather difficult to compel cooperation among nations. This pact contains a great number of loopholes, which makes it possible for criminals to continue committing crimes. It is needed that an increasing number of nations join this treaty and adopt national laws, as well as keep on updating the rules in accordance with new sorts of crimes, in order to have a treaty that is more effective and efficient.

You are Moitra, S. D (2005), investigate in this research that there are a variety of concerns that are extremely significant for the creation of policies related to cyber crimes[10]. This is something that is very important for the development of policies. The many worries or problems may be organized into five questions, which are as follows: 1.Criminals 2.Crimes 3.The occurrence of cybercrime 4.The effect on victims and 5.What can be done about it.

5.The reaction of the society. This research also delves into the reasoning behind why each concern should be taken into account when formulating policy. In 2001, the Europe Council ratified its Agreement on Cybercrime, and since then, the European Union has initiated a variety of programs to combat online criminal activity. The need for standardization and coordination in order to arrive at a universal taxonomy of cybercrime is another topic that is covered in this paper. Before developing laws and regulations for cyber law, it is necessary to do in-depth research on a variety of factors, including the behavior of hackers, the reactions of victims, legal activities, and policies governing criminal justice. Although rules still exist in several nations including the United States, the Agreement on Cybercrime (EU), and the Information Technology Act of 2000, ongoing research into cybercrime is important since new issues may arise in the future and new forms of cybercrimes may emerge. Although these policies do exist, they will need to be upgraded on a timely basis. The findings indicate that credible information have to be gathered and analyzed prior to the formulation of brand-new policies. The suggestions that are provided in this research might also be of use to those nations which are still in the process of developing their policies. This research does have a few flaws, such as the fact that it does not cover all relevant aspects and there are still a great many additional considerations to take into account.

The authors' names are Oriwoh, E.; Sant, P.; and Epiphaniou, G. (2013) propose a set of guiding principles for vendors, customers, governments, and legislators that collaborate with or utilize the Internet of Things (IoT) [11]. In most cases, new technologies and novel applications of already existing technologies shed light on potential future uses and appropriate applications for the technology in question. Multiple experts have recognised the significance of security concerns in the early stages of the development of any technologies related to the internet of things (IoT).

There are currently regulations in place, and new laws also give direction to the users of IoT and guarantee that there should not be any fraud or breach in the utilization of technologies; if it is discovered, then appropriate action should be taken to chastise the offender [47]. As a result, it is essential that proper guidelines for guiding be developed and implemented in order to provide the laws to the users who are interested in them.

Not to be outdone, Maung, T. M., and Thwin, M. M. S. (2017) came to the conclusion that new and updated operating systems bring up new difficulties in the field of forensic cybercrime investigation [12]. On the one hand, newer versions of Windows make things simpler for computer users, but on the other, they can open up the door to new criminal opportunities. The field of cybercrime forensics is not a new one; yet, in order to successfully identify cybercriminals, it is essential that this field continually upgrade its investigative techniques. Experts in computer forensics conduct investigations into computer crimes based on the principles of quality, efficacy, legal requirements, and flexibility. The objective of the investigation needs to be tailored, expertised, methodical, and thorough enough to ensure that the process of inquiry is finished in a shorter amount of time and that pertinent information may be obtained and researched accordingly[44]. The term "digital evidence" refers to the digital data that demonstrates that a crime has been committed and that there is a connection between the victim and the crime or between the criminal and the crime. The Internet of Things is susceptible to a wide variety of threats and malware's, including viruses, spies, worms, and Trojan horses, which impact it virtually on a daily basis [40]. IT security is highly challenging in this digital environment. This new research reveals a variety of strategies that, when used methodically, can result in the collection of reliable forensic evidence. These solutions provide assistance and support in the process of gathering apparent information in a variety of forensic sectors, including cloud, static, and social network [25]. The primary purpose of this research is to arrive at a recommendation that is suitable for the nation of Myanmar.

THERE ARE THREE DIFFERENT TYPES OF CYBER ATTACKS ON IoT DEVICES

Attacks of the Physical Kind:

When an Internet of Things device is accessed in the traditional sense, it opens the door to the possibility of a physical attack. This sort of assault may be carried out by a single employee of the same organization who has access to the Internet of Things device.

Methods of Attacking Encryption:

When an Internet of Things device is not encrypted, an encryption attack is possible because an attacker can sniff the data with the assistance of an intruder. Attacks against encryption target the most essential components of your algorithmic infrastructure. Hackers examine and derive the meaning of your encryption keys in order to determine how you generate such algorithms. After the encryption keys have been decrypted, the machine can be taken over by cybercriminals who can then install their own algorithms and use them to their advantage.

Attacks Using the DoS (Denial of Service) Protocol:

It's possible that an assault of this type wouldn't take data from services like webpages [24]. Attackers target services by using a large number of botnets to send thousands of requests to the targeted services, which causes the services to crash and makes the targeted services inaccessible.

Hijacking of the Firmware:

When an Internet of Things device is not kept up to date, it leaves itself vulnerable to assaults of the firmware variety. Attackers have the ability to take control of the device and install malicious software. Computers have a variety of different kinds of firmware, and all of them is theoretically susceptible to being hacked.

Attacks Via Botnet:

An assault known as a botnet attack may be carried out when an Internet of Things device is converted into a remotely controlled bot that can then be employed as a component of the botnet. It is possible for botnets to join to the network and transfer the sensitive and private information. There are two distinct kind of botnet assaults: the Mirai botnet and the PBot virus.

Attack Using a Man in the Middle:

When a hacker monitors the communication taking place between two systems, they are able to launch an attack known as man in the middle. by listening in on the conversation that is taking place between the two parties [17]. The Man in the Middle attack can take one of seven different forms, including the following: a) IP spoofing; b) DNS spoofing;

c) Spoofing HTTPS; d) Hijacking SSL; e) Hijacking email; f) Eavesdropping on wireless networks via Wi-Fi;

g) Theft of cookies from a browser

Attacks Using Ransomware

Ransomware is a sort of attack in which the data are encrypted and the access is locked down by the cybercriminal. The hacker will then sell the decryption for the fee that he has set. This sort of assault will make normal corporate operations difficult to carry out [51]. Scareware, screen locks, and encrypting ransomware are the three types of attacks that fall under the ransomware umbrella.

Attack Based on Eavesdropping:

When a hacker intercepts network communication in order to get access to sensitive and confidential data via a weekend link between an Internet of Things device and a server, this type of attack is known as eavesdropping [35]. The use of a personal firewall, keeping antivirus software up to date, and making use of a virtual private network are all ways that an eavesdropping assault might be prevented.

Attacks That Escalate in Privilege Level:

In this type of cyberattack, the hacker hunts for vulnerabilities in Internet of Things (IoT) devices so that they may acquire access. During this particular assault, the utilize their recently acquired credentials to spread malware. A hacker gains elevated access to resources that a third party should typically be unable to access by exploiting a defect, design flow, or configuration error in an application or operating system. This access would normally be inaccessible to the third party.

Brute-Force Attempt to Guess Your Password:

In the course of the assault, the hacker will utilize password hashing or password cracker software in order to bombard the server with as many possible attempts as they can muster. Up until the time when the hacker has the necessary credentials. The approach of trial and error is utilized by the hacker in order to guess login passwords, encryption keys, or locate hidden web sites. Different kinds of assaults using brute force include: a) simple brute force attacks. b) Attacks using dictionaries; c) Attacks using hybrids of brute force and brute force; d) Attacks using brute force in reverse; and e) Attacks using credentials stuffing.

SMART HOME IN ADDITION TO ALL OF ITS SUBSYSTEMS

If one of the devices in your smart home is vulnerable and unencrypted, your data will be on Networks like Google dorks and Shodan, which are the first places that hackers look for information [13]. Smart homes are equipped with advanced automated internet-connected devices that make your life much easier, such as multimedia kits, automatic door and window operators, smart home appliances, and so on. Most of the time, the physical components, the communication system, and the intelligent information processing are the three most significant aspects that are included in the smart home appliances. Which company manufactures the most cutting-edge intelligent home products.

Because IoT-based smart home gadgets are extremely vulnerable to attack in comparison to other devices [36], bringing Internet of Things technology into our home will bring about an increase in the number of security problems and challenges we face. If the smart home device is attacked and its security is breached, there is a possibility that the user's privacy will be invaded, personal information will be stolen, and the user will be observed [14].

THE PRESENT APPROACHES FACE THE FOLLOWING CHALLENGES

The Downsides of Testing:

IoT devices are susceptible to cyberattacks because they do not undergo appropriate testing and do not receive frequent software updates. There are already over 30 billion devices that are linked to the internet. Some manufacturers of Internet of Things devices provide firmware upgrades, but regrettably, these devices are vulnerable to cyberattacks since they do not get automated updates, as reported by zero-day hacks[43].

Passwords Set by Default:

According to certain government studies, manufacturers should be warned against selling Internet of Things devices with the default credentials (admin and password) [46]. The Internet of Things devices that have weak passwords or default passwords have been identified as the most vulnerable devices to password cracking and brute-force attacks.

Internet of Things Ransomware:

Encryption is necessary for the ransomware in order to prevent access to users on a variety of devices and platforms [34]. There is a chance that ransomware will protect the device from an assault, but in the long run, a hacker will be able to encrypt part of the user's personal data using the software.

IoT:

AI and automation are dependent on the volume of data collected by sensors and the internet of things. Is always growing to huge proportions. In the process of moving enormous amounts of information from one network to another, AI technologies and automation have previously been employed. The use of these AI tools to make autonomous judgments, on the other hand, has the potential to impact millions of functions throughout infrastructure, including those related to healthcare and transportation, among other areas [29], [48].

Botnet Attacks:

A botnet attack is when a hacker develops a collection of malware-infected botnet and sends thousands of requests per second in an effort to knock down the target [16]. There is a possibility that a single Internet of Things device compromised with malicious code or malware does not pose a significant hazard [19]. When a hacker utilizes DDoS assaults, thousands of IP cameras, home routers, and other smart devices can be hacked and used to knock down DSN provider platforms like Netflix and GitHub [42].

III. CONCLUSION

In today's hyper-connected society, the Internet of Things has quickly become one of the most vital topics for all people. The Internet of Things (IoT) is making the globe seem smaller. The internet has brought the entire human race closer together and connected them to one another. Because of the proliferation of online transactions, the incidence of criminal activity has increased. The extent of criminal activity in cyberspace is quite broad and is not limited to a particular geographic place or nation. It is impossible to overlook the risks associated with cyber assaults; thus, it is essential to take appropriate precautions while implementing IoT on a daily basis. Installing software protection such as a firewall, anti-virus software, and anti-malware software are all simple actions that consumers may do to increase their level of security. It is important to educate people about the many forms of cybercrime that might occur in the IoT as well as the preventative measures that can be taken. Controlling cybercrime requires the implementation of a number of international conventions. The idea and substance of the many multilateral, municipal, and national legal devices and laws that are in effect today, as well as their scope of criminalization and inquiry, are all distinct.

capabilities and techniques, digital evidence, risk and laws, and international control and cooperation are among of the topics covered. The geographical scope of these accords, such as multilateral or regional, as well as their applicability, are both distinct from one another. Because of these variations, identifying cybercriminals, conducting investigations of them, taking legal action against them, and adopting preventative actions about cybercrime can be difficult. Therefore, the only way to ensure that the Internet of Things (IoT) is governed in accordance with the same set of rules everywhere and that there is no room for ambiguity is to forge international treaties that are multilateral, cooperative, and adaptable. Criminals who commit crimes online should face severe penalties, and other people who could commit crimes themselves should be deterred as a result. It should guarantee that the rules that are enacted must be properly obeyed, and limits, if any, that are put on internet access and content should not be ignored [31]. The law and the rights of persons ought to be taken into consideration while drafting these laws [41]. It is difficult to develop uniform worldwide rules because of the breadth and effect of cyber laws in various nations. For example, if a piece of material on the internet is legal in one country but not in another, the challenge is caused by the fact that some governments have legalized the content while others have not.

IV. REFERENCES

[1]. Yang Lu and Li Da Xu, (2019) Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics, IEEE Internet of Things Journal ,Volume: 6 , Issue: 2 , pp- 2103 – 2115.

[2]. Hilt, S.; Kropotov, V.; Merces, F.; Rosario, M. and Sancho, D. (2017) The Internet of Things in the Cybercrime underground, Trend Micro Research,pp-1-46

[3]. Dr. Venckauskas, A.; Dr. Damasevicius,R.; Dr. Jusas, V.; Dr. Toldinas, J.; Rudzika, D.and Dregvaite, G. (2015), A Review Of Cyber-Crime In Internet Of Things: Tech- nologies, Investigation Methods And Digital Forensics, International Journal Of En- gineering Sciences Research Technology, Venckauskas, 4(10):Pp-460-477

[4]. Abomhara, M. and Koien, G. M. (2015) Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal of Cyber Security, Vol. 4, 65–88.

[5]. J. Iqbal and B. M. Beigh,(2017),Cybercrime in India: Trends and Chal- lenges, International Journal of Innovations Advancement in Computer Science, Volume 6, Issue 12,pp-187-196.

[6]. Sarmah, A.; Sarmah, R. and Baruah, A. J. (2017),A brief study on Cyber Crime and Cyber Law's of India, International Research Journal of Engineering and Tech- nology, Volume: 04 Issue: 06, pp-1633- 1641

[7]. MS. Anisha (2017)Awareness And Strategy To Prevent Cybercrimes: An Indian Perspective, Indian Journal Of Applied Research, Volume - 7 — Issue – 4, Pp-114- 116.

[8]. Husamuddin, M.; Qayyum, M. (2017), Internet of Things :A Study on Security and Privacy Threats, : The 2nd International Conference on Anti-Cyber Crimes (ICACC) organized by IEEE.

[9]. Marion, N. E. (2010) The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. International Journal of Cyber Criminology, Vol. 4 Issue 12, pp-699–712.

[10]. Moitra, S. (2005). Developing Policies for Cyber crime, European Journal of Crime, Criminal Law and Criminal Justice, 13(3), 435-46.

[11]. Oriwoh, E.; Sant, P. and Epiphaniou, G. (2013) Guidelines for Internet of Things deployment approaches – The Thing Commandments, The 4th International Con- ference on Emerging Ubiquitous Systems and Pervasive Networks, pp- 122- 131

[12]. Maung, T. M.; Thwin, M. M. S. (2017), Proposed Effective Solution for Cybercrime Investigation in Myanmar, The International Journal Of Engineering And Science, Volume – 6, Issue-1, PP 01-07

[13]. Anthi, E., Williams, L., Slowi nska, M., Theodorakopoulos, G., Bur- nap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT devices. IEEE Inter- net of Things Journal.

[14]. P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, L. Maddox, O. Santos, and R. M. Montalvo, "Cyber risk from IoT technologies in the supply chain – discussion on supply chains decision support system for the digital economy," Oxford, 2019.

[15]. K. Carruthers, "Internet of Things and Beyond: Cyber-Physical Systems- IEEE Internet of Things," IEEE Internet of Things, Newsletter, 2014, 2016.

[16]. Lipman Paul, "New Reaper IoT Botnet Leaves 378 Million IoT Devices Potentially Vulnerable to Hacking," 2017.

[17]. K. Savage, "IoT Devices Are Hacking Your Data amp; Stealing Your Privacy - Infographic," 2017.

[18]. 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, 2013.

[19]. Schiefer, M. (2015, May). Smart Home Definition and Security Threats. In IT Secu- rityincident Management ITForensics(IMF), 2015 Ninth International Conference on (pp. 114-118). IEEE.

[20]. Tong, J., Sun, W., Wang, L. (2013, May). An information flow security model for home area network of smart grid. In Cyber Technology in Automation, Control and Intelligent Systems (CYBER), 2013 IEEE 3rd Annual International Conference on (pp. 456-461). IEEE.

[21]. Padyab, A. M., Paivarinta, T., Harnesk, D. (2014, January). Genre- Based Assess- ment of Information and Knowledge Security Risks. In System Sciences (HICSS), 2014 47th Hawaii International Conference on (pp. 3442-3451). IEEE.

[22]. McCune, J. M., Perrig, A., Reiter, M. K. (2005, May). Seeing-is- believing: Using camera phones for human-verifiable authentication. In Security and privacy, 2005 IEEE symposium on (pp. 110-124). IEEE.

[23]. Madakam, S., Ramaswamy, R., Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3(05), 164.

[24]. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, vol. 35, no. 10, pp. 54–62, 2002.

[25]. D. G. Holmberg, "BACnet Wide Area Network Security Threat Assessment", Tech- nical report, National Institute of Standards and Technology, 2003.

[26]. Ch, R., Gadekallu, T. R., Abidi, M. H., Al-Ahmari, A. (2020). Computational System to Classify Cyber Crime Offenses Using Machine Learning. Sustainability, 12(10), 4087.

[27]. Maddikunta, P. K. R., Srivastava, G., Gadekallu, T. R., Deepa, N., Boopathy, P. (2020). Predictive model for battery life in IoT networks. IET Intelligent Transport Systems.

[28]. RM, S. P., Maddikunta, P. K. R., Parimala, M., Koppu, S., Reddy, T., Chowdhary, C. L., Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Computer Communica- tions.

[29]. Deepa, N., Prabadevi, B., Maddikunta, P. K., Gadekallu, T. R., Baker, T., Khan, M. A., Tariq, U. (2020). An AI based intelligent system for healthcare analysis using Ridge Adaline Stochastic Gradient Descent Classifier. Journal of Supercomputing.

[30]. Maddikunta, P. K. R., Gadekallu, T. R., Kaluri, R., Srivastava, G., Parizi, R. M., Khan, M. S. (2020). Green communication in IoT networks using a hybrid optimization algorithm. Computer Communications.

[31]. RM, S. P., Bhattacharya, S., Maddikunta, P. K. R., Somayaji, S. R. K., Laksh- manna, K., Kaluri, R., ... Gadekallu, T. R. (2020). Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. Journal of Parallel and Distributed Computing.

[32]. Iwendi, C., Jalil, Z., Javed, A. R., Reddy, T., Kaluri, R., Srivastava, G., Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks. IEEE Access, 8, 72650-72660.

[33]. Numan, M., Subhan, F., Khan, W. Z., Hakak, S., Haider, S., Reddy, G. T., ... Alazab, M. (2020). A

systematic review on clone node detection in static wireless sensor networks. IEEE Access, 8, 65450-65461.

[34]. Patel, H., Singh Rajput, D., Thippa Reddy, G., Iwendi, C., Kashif Bashir, A., Jo, O. (2020). A review on classification of imbalanced data for wireless sensor networks. International Journal of Distributed Sensor Networks, 16(4), 1550147720916404.

[35]. Reddy, T., RM, S. P., Parimala, M., Chowdhary, C. L., Hakak, S., Khan, W. Z. (2020). A deep neural networks based model for uninterrupted marine environment monitoring. Computer Communications.

[36]. Iwendi, C., Maddikunta, P. K. R., Gadekallu, T. R., Lakshmanna, K., Bashir, A. K., Piran, M. J. (2020). A metaheuristic optimization approach for energy efficiency in the IoT networks. Software: Practice and Experience.

[37]. Bhattacharya, S., Kaluri, R., Singh, S., Alazab, M., Tariq, U. (2020). A Novel PCA- Firefly based XGBoost classification model for Intrusion Detection in Net- works using GPU. Electronics, 9(2), 219.

[38]. Azab, A., Layton, R., Alazab, M., Oliver, J. (2014, November). Mining malware to detect variants. In 2014 Fifth Cybercrime and Trustworthy Computing Conference (pp. 44-53). IEEE.

[39]. Alazab, M., Layton, R., Broadhurst, R., Bouhours, B. (2013, November). Malicious spam emails developments and authorship attribution. In 2013 Fourth Cybercrime and Trustworthy Computing Workshop (pp. 58-68). IEEE.

[40]. Bali, R. S., Kumar, N. (2016). Secure clustering for efficient data dissemination in vehicular cyber–physical systems. Future Generation Computer Systems, 56, 476- 492.

[41]. Chaudhary, R., Kumar, N., Zeadally, S. (2017). Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges. IEEE Communications Magazine, 55(11), 114-122.

[42]. Singh, A., Maheshwari, M., Kumar, N. (2011, April). Security and trust manage- ment in MANET. In International Conference on Advances in Information Technol- ogy and Mobile Communication (pp. 384-387). Springer, Berlin, Heidelberg.

[43]. Vora, J., Italiya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., Hsiao, K. F. (2018, July). Ensuring privacy and security in E-health records. In 2018 Interna- tional conference on computer, information and telecommunication systems (CITS) (pp. 1-5). IEEE.

[44]. Hathaliya, J. J., Tanwar, S., Tyagi, S., Kumar, N. (2019). Securing electronics healthcare records in healthcare 4.0: a biometric-based approach. Computers Elec- trical Engineering, 76, 398-410.

[45]. Krishnasamy, L., Dhanaraj, R. K., Ganesh Gopal, D., Reddy Gadekallu, T., Aboudaif, M. K., Abouel Nasr, E. (2020). A Heuristic Angular Clustering Frame- work for Secured Statistical Data Aggregation in Sensor Networks. Sensors, 20(17), 4937.

[46]. Mohan Vijay (2018). AN UPDATED NEW SECURITY ARCHITECTURE FOR IOT NETWORK BASED ON SOFTWARE-DEFINED NETWORKING (SDN). IRJCS:: International Research Journal of Computer Science, Volume V, 77-81.

[47]. Krishna Kagita, M. (2019). Security and Privacy Issues for Business Intelligence in a loT. In Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019 [8688023]

[48]. Krishna Kagita, M. and M. Varalakshmi, 2020. A detailed study of security and privacy of Internet of Things (IoT). International Journal of Computer Science and Network, 9 (3): 109–113.

[49]. Navod Neranjan Thilakarathne, Mohan Krishna Kagita, Dr. Thippa Reddy Gadekallu. (2020). The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study. International Journal of Engineering and Management Research, 10(4), 145-159.

[50]. Alazab, M., Venkatraman, S., Watters, P., Alazab, M. (2013). Information se- curity governance: the art of detecting hidden malware. In IT security

governance innovations: theory and research (pp. 293-315). IGI Global.

[51]. Farivar, F., Haghighi, M. S., Jolfaei, A., Alazab, M. (2019). Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE transactions on industrial infor- matics, 16(4), 2716-2725.

[52]. Azab, A., Alazab, M., Aiash, M. (2016, August). Machine learning based botnet identification traffic. In 2016 IEEE Trustcom/BigDataSE/ISPA (pp. 1788-1794). IEEE.

[53]. Alazab, M., Huda, S., Abawajy, J., Islam, R., Yearwood, J., Venkatraman, S., Broadhurst, R. (2014). A hybrid wrapper-filter approach for malware detection. Journal of networks, 9(11), 2878-2891.

[54]. Garg, S., Singh, A., Batra, S., Kumar, N., Yang, L. T. (2018). UAV-empowered edge computing environment for cyber-threat detection in smart vehicles. IEEE Network, 32(3), 42-51.

Cite this article as :

Dinker Kumar, Vinod Mahor, "A Review : Cyber Crime", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.693-705, March-April-2023.