IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

A Review on Internet of Things

Priyarani A G, Priyanka R, Priyanka V K, Punya N, Priya D B, Rachana Nayak
Students 3rd Semester, Department of Computer Science and Engineering
Alva's Institute of Engineering and Technology, Moodabidire, Dakshina Kannada, Karnataka, India

Abstract: *As the Internet of Things (IoT) develops as the next phase in the Internet's growth, it's critical to identify the numerous potential domains of IoT applications and the research agenda connected with these applications. Become. The Internet of Things is predicted to transform everything from smart cities to smart agriculture, logistics, retail, smart homes, and smart ecosystem permeate almost every aspect of everyday life. Today's IoT technology has improved significantly over the last few years, but there are still many issues that need attention. As the concept of IoT emerges from heterogeneous technologies, many research challenges inevitably arise. The fact that the IoT is so widespread that it affects almost every area of our lives has become a significant research topic for research in various related areas such as information technology and computer science. Therefore, the IoT opens the way to a new dimension in research. This white paper describes recent developments in IoT technology and addresses future application and research challenges.*

Keywords: Internet of Things

I. INTRODUCTION

The Internet is a communication network that allows people to connect to information. On the other hand, the Internet of Things (IoT) is a globally addressable physical object interconnect system with interoperability and sharing capabilities, as well as individual processing, detection, and activation capabilities. As a common platform for communication, shared use uses the Internet. Therefore, the main goal of the Internet of Things is to allow objects to connect via any network, path, or service to other objects, people, anytime, anywhere. The Internet of Things (IoT) is beginning to be seen as the next step in the evolution of the Internet. The IoT will allow regular devices to connect to the Internet to achieve a myriad of different goals. Currently, it is estimated that only 0.6% of devices that can participate in the IoT are networked. However, by 2020, more than 50 billion devices are expected to be connected to the Internet.

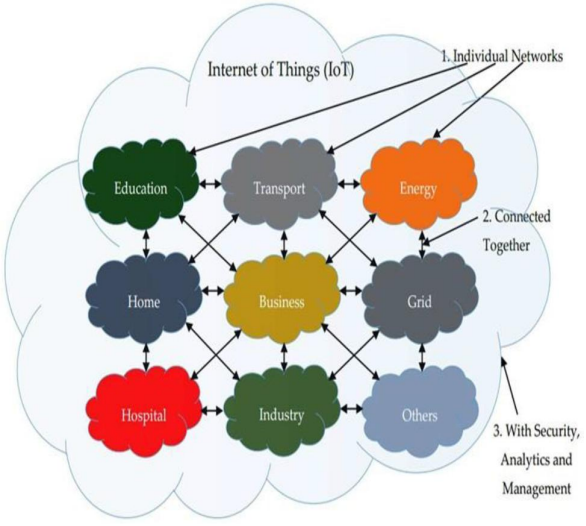

Figure 1: IoT can be viewed as a Network of Networks

As the Internet has evolved, it has become more than just a network of computers, it has become a network of various devices. The IoT, on the other hand, acts Figure 1 depicts a network of networks as a collection of several "connected" devices. Smartphones, vehicles, industrial systems, cameras, toys, buildings, home appliances, industrial systems, and a plethora of other Internet-connected devices are examples of devices. These devices can perform intelligentre organization,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

tracking, positioning, control, real-time monitoring, and process control regardless of size or function. There has been a tremendous increase in the number of internet-enabled devices in recent years. Its most important commercial impact has been observed in the consumer electronics sector, which means that connecting people, especially with the smartphone revolution and interest in wearable devices (watches, headsets, etc.), brings the digital and physical worlds together. It's just part of the bigger move to connect.

With this in mind, the Internet of Things (IoT) is expected to continue expanding its reach in terms of the number of gadgets and functions it can support. The paradox inside the expression "Things" demonstrates this, making it difficult to describe the IoT's ever-evolving limitations. While industrial fulfilment continues to materialize, the Internet of Things (IoT) continues to provide an almost limitless supply of possibilities, not only in groups but also in studies. As a result, the understudy examines a variety of capability areas for software of IoT domain names, as well as challenging situations that may be associated with those applications.

II. GROWTH OF IOT

Internet has been component and parcel of the social animal`s life. It`s a large area of facts and humans. The net first advanced as “net of computers”. It is an international platform wherein many offerings just like the World Wide Web can be carried out on pinnacle of it. It changed into a generation of facts exchange. As the times surpassed through, humans commenced rising into the net- “Internet of humans”. Many social web sites got here into photo which stored humans linked all of the time. This has caused net being full of humans in place of facts. On the opposite hand, generation has been advancing daily and concurrently a generation of “MobiComp” (cellular computing) had begun. Mobile helped guy to be continually linked to the net at the move. Nowadays 3G and 4G cellular net connections have caused quicker net get admission to and supply higher great in video calls. Wireless technology and cellular computing have turn out to be reasonably-priced and feature received greater popularity [5]. Hence a brand new computing had emerged- Ubiquitous computing. This computing makes a speciality of clever, shrewd area and minimum consumer involvement.

Advancement in generation caused cellular and different hand held gadgets to decrease in size. Smart telephones, Ipads, pills and notebooks changed normal mobiles and PCs. Hence there has been an alternate withinside the tool with which humans get admission to the net. This inturn ended in state-of-the-art capabilities being configured in gadgets which includes sensors, Global Positioning system (GPS) and actuators. In this sort of state of affairs gadgets have been now no longer best linked to the net however additionally sense, compute and carry out shrewd tasks. Later bodily gadgets have been configured with identity tags which includes bar code and RFID in order that they can be scanned through gadgets like clever telephones and add their facts into the net. This manner of connecting the bodily international with our on-line world with the assist of a clever tool caused net being referred to as as “Internet of Things”. Hence IOT has its roots from Mobile computing, ubiquitous computing and facts generation.

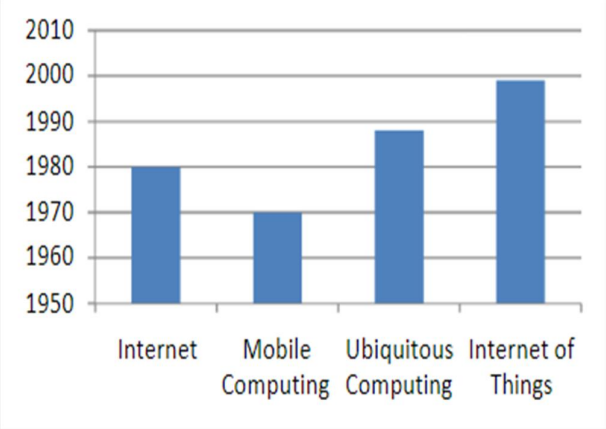

Figure 2: Growth of IoT

IOT connects the gadgets in a shrewd manner. The “thing” right here refers back to the bodily item`s facts study thru sensors and RFID reader and uploaded into the net. The bodily item may be something from clever telephones to gadgets at home. The International telecommunications Union (ITU) has mentioned 4 dimensions of an IOT : item identity (“ tagging

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

matters") , sensors and wi-fi sensor networks(" feeling matters"), embedded systems ("wondering matters") and nanotechnology ("shrinking matters`). Hence from the above , IOT adjustments the connectivity view from "any-time , any-place" for "any-one" into "any-time , any-place" for "any-thing". These matters as soon as linked to the net offer clever offerings useful to the surroundings and society. They play a prime function in deliver chain, energy, defence, fitness care and different beneficial applications.

III. APPLICATIONS OF IOT

The Internet of Things' applications are not only many, but also diversified, as they touch practically every element of people's, institutions', and societies' daily lives. As a result, IoT applications span a wide range of industries, including manufacturing, healthcare, agriculture, smart cities, security, and disaster relief.

3.1 Smart City

According to the IoT, it will play a key role in making cities smarter and improving the overall infrastructure. Areas of IoT applications in creating smart cities include smart transportation systems, smart construction, congested waste management, smart lighting, smart parking, and city maps. This can include various features such as: Monitor available parking spaces in the city, monitor the vibration and physical condition of bridges and buildings, install noise monitoring devices in sensitive areas, and monitor pedestrian and vehicle levels. The IoT enabled by artificial intelligence (AI) can be used to monitor, control, and reduce traffic congestion in smart cities. In addition, the IoT will enable theinstallation of intelligent, weather-adaptive street lighting, as well as the identification of recycle bins and bins by following the garbage collection schedule. Smart roadways can give crucial information and alarms such as: B. Access to detours in the event of adverse weather or unforeseen incidents such as traffic congestion or accidents. The usage of radio frequency identification and sensors is required to implement IoT in the creation of smart cities. Aware Home and Smart-Santander are two applications that have previously been developed in this field. Several large cities in the United States, including Boston, are working on ways to integrate the Internet of Things into nearly every infrastructure, from parking meters to street lighting, sprinklers, and sewer grate. All of these are linked to the internet and are interlinked.

3.2 Healthcare

It is a term that refers to the provision of medical services. Many countries' healthcare systems are inefficient, slow, and prone to mistakes. Because the healthcare industry relies on multiple activities and gadgets that technology can automate and enhance, this can simply be modified. Additional technologies that facilitate a variety of tasks, such as sharing reports with various individuals and locations, storing records, and administering medicines, would significantly aid the healthcare sector's transformation. Patient, staff, and asset tracking, person identification and authentication, and automatic data collecting and collection are just a few of the advantages that IoT applications offer in health. The ability to track patient flow can greatly enhance hospital workflows. Authentication and identity also decrease occurrences that could endanger the patient, as well as record keeping and newborn mismatch. Furthermore, automated data collection and submission is important for process automation, reduced form processing time, automated procedure reviews, and medical inventory management. Sensor devices enable patient-centric functionality, especially when diagnosing conditions and leveraging real-time information about patient health indicators.

The realization of the Internet of Things (IoT) and Internet of Things (IoE) applications enhances the Internet of Things (IoT) and Internet of Things (IoE) applications [3]. As the name implies, the term IoNT refers to the use of nanonetworks to integrate nano sensors into various objects (things). Medical applications are one of the key focal points of IoNT implementations, as seen in Figure 2. When IoNT is applied to the human body for therapeutic reasons, access to data from in-situ regions of the body that were previously inaccessible to or not detectable by or employing cumbersome sensor-sized medical devices improves. As a result, IoNT will enable the collection of new medical data, resulting in novel discoveries and improved diagnostics.

3.3 Intelligent Agriculture and Water Management

The IoT has the ability to empower and improve the agricultural sector by investigating soil moisture and, in the case of vineyards, monitoring the diameter of the stem. The Internet of Things allows us to control and store the amount of vitamins

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

in agricultural products and adjust microclimate conditions to maximize the production and quality of vegetables and fruits. In addition, studying weather conditions can predict ice information, droughts, wind changes, rain and snow, and control temperature and humidity levels to prevent fungal and other microbial contamination.

For cattle, the IoT can help identify animals grazing in open areas, detect harmful gases in farm animal excrement, and control the growth conditions of offspring to improve health and survival potential. It will help. In addition, through IoT applications in agriculture, a lot of waste and corruption can be avoided through proper monitoring technology and management of the entire agricultural sector. It also leads to better power and water control.

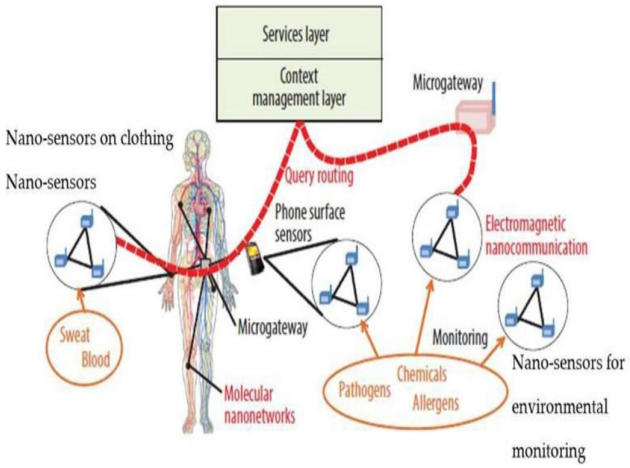

Figure 3: The Internet of Nano-Things

The role of IoT is to investigate the compatibility of sea and river water for both drinking and agriculture, detect pressure fluctuations in pipes and the presence of liquids outside tanks, and monitor water fluctuations in dams, rivers and reservoirs. It is included. These IoT applications use wireless sensor networks. Examples of existing IoT applications in this area are SiSviA, GBROOS and SEMAT.

IV. Retail And Logistics

There are many benefits to running the IoT in supply chain or retail management. Some are included. Monitoring storage status throughout the supply chain, product tracking that enables traceability, and payment processing based on location or duration of activity in public transport, amusement parks, gyms, etc. Within the retail store, the IoT can be applied to a variety of applications, including: B. In-store guidance based on preselected lists, automated checkout using biometrics, detection of potentially allergic products, control of product rotation in shelves and warehouses to automate the replenishment process, etc. Rapid payment process.

The most commonly used IoT elements in this environment include wireless sensor networks and radio frequency identification. While retailers are currently using SAP (system applications and products), logistics has many examples such as quality of shipping conditions, location of items, detection of warehouse incompatibilities, fleet tracking, and more. I have. In the industry, IoT detects gas and leaks in and around the industry, tracks toxic and oxygen concentrations within the boundaries of chemical plants, ensures the safety of goods and workers, and monitors gas concentrations. Helps to. Water in water tanks and storage tanks. IoT applications are also useful for maintenance and repair because you can configure your system to anticipate device malfunctions while automatically scheduling regular maintenance services before equipment failures occur. This can be achieved by installing sensors on the device or machine, monitoring their capabilities, and possibly sending reports.

V. Intelligent Life

In this area, IoT can be applied to remote control devices to remotely turn the device on and off, preventing accidents and saving energy. Other smart home devices include refrigerators with LCD (Liquid Crystal Display) screens, what is available inside, what is exhausted, what is out of date, and what needs to be replenished. You can know if there is one. You can also link this information to a smartphone application so that people can access it outside the home and buy what they need. In

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

addition, the washing machine can enable remote monitoring of the laundry. In addition, you can connect various kitchen appliances with your smartphone and control the temperature like an oven. Some ovens with self-cleaning capabilities are easy to monitor. In terms of home security, the IoT can be applied through alarm systems and cameras can be installed to monitor and detect window and door openings, preventing intruders.

VI. Smart Environment

The environment plays an important role in every aspect of life, from humans to animals, birds to plants. All of these are somehow affected by the unhealthy environment. Although much effort has been made to create a healthy environment to eliminate pollution and reduce waste of resources, the presence of industry and transportation waste combined with reckless and harmful human behavior has always been present. It is an everyday element that damages the environment.

As a result, the environment needs intelligent and innovative methods to support waste monitoring and management, providing large amounts of data that force governments to set up systems to protect the environment. .. We need to develop smart environmental strategies integrated with IoT technology to collect, track and evaluate environmental objects that have potential benefits for sustainable living and the green world. IoT technology enables air quality monitoring and management by collecting data from urban remote sensors and providing 24/7 geographic coverage to better manage congestion in major cities. In addition, IoT technology can be used to measure water pollution levels, facilitating water usage decisions. IoT can be applied to waste management, which consists of various types of waste that are harmful not only to the environment but also to humans, animals and plants, such as chemicals and pollutants. This can be achieved through environmental protection by managing industrial pollution through an immediate monitoring and management system in combination with monitoring, in addition to the decision-making network. This helps to avoid waste.

Weather forecasts can use the IoT to provide high accuracy and high resolution for weather monitoring through information sharing and data sharing. Through IoT technology, meteorological systems can collect information such as barometric pressure, humidity, temperature, light, and movement from moving vehicles and send that information wirelessly to meteorological stations. Information is obtained by installing sensors in vehicles and buildings and then stored and analyzed for use in weather forecasts. Radiation is also a threat to the environment, human and animal health, and agricultural productivity. IoT sensor networks can control radiation, detect leaks and spread deterrence by constantly monitoring their levels, especially around the site of a nuclear power plant.

VII. Drawbacks of IoT Devices

In recent years, the use of the Internet of Things (IoT) has increased dramatically, raising concerns about cybersecurity. It increased with it. At the forefront of cybersecurity is artificial intelligence (AI), which is used to develop complex algorithms to protect networks and systems, including IoT systems. However, cyber attackers understand how to exploit AI and start using enemy AI to launch cyber security attacks. This review paper also has a compilation of information from several other research and research papers on IoT, AI, and attacks. It is intended to oppose AI, examine the relationships between these three topics, and comprehensively present and summarize relevant literature in these areas.

Since the birth of the Internet of Things (IoT) around 2008, its growth has been booming, and IoT is now a part of everyday life and is used by many homes and businesses. The IoT is difficult to define because it has evolved and changed since its inception, but it has unique identifiers (UIDs) and can exchange data with digital and analog machines without human intervention. Best understood as a network of devices. Most often, this manifests itself as a human interface with a central hub device or application (often a mobile app), where the mobile app sends data and instructions to one or more edge IoT devices. Edge devices can perform functions as needed and send data back to hub devices or applications for human viewing. The concept of the IoT has brought a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability to the world when it comes to device connectivity. However, the IoT is vulnerable to cyberattacks due to the combination of multiple attack surfaces and their novelty, and the resulting lack of security standards and requirements.

Cyber-attacks that attackers can use against the IoT vary depending on which aspect of the targeted system and what the attack wants to achieve. Therefore, much research is being done on cyber security surrounding the IoT. This includes an artificial intelligence (AI) approach to protect IoT systems from attackers. This is usually from the perspective of detecting anomalous behavior that may indicate an attack. However, with the IoT, cyber attackers only need to find one vulnerability, and cyber security experts need to protect multiple targets, so they are always in the lead. This has increased the use of AI,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

including cyber attackers, to prevent advanced algorithms that detect anomalous activity and pass unnoticed. AI is receiving a lot of attention as IoT technology grows. This overview paper covers a variety of topics related to cybersecurity, the Internet of Things (IoT), and artificial intelligence.

AI and all of them interrelationships, in three research style sections, provide a comprehensive overview of cyberattacks targeting IoT devices and recommended AI-based methods to protect against these attacks. Offers. The ultimate goal of this paper is to create resources through presentations for others investigating these common issues.

7.1 Methods of Attacking IoT Devices

Due to the loose security of many IoT devices, cyber attackers have found many ways to attack IoT devices from different attack surfaces. Attack surfaces range from both hardware and software IoT devices themselves to networks. The application to which the IoT device is connected and the application to which the device is connected. They are the most three Attack surface commonly used to form the key components of IoT systems. Common IoT system failures. Most of the attacks described in this document occur at network gateways. Cloud data server connection. These connections are where IoT security is most lacking.

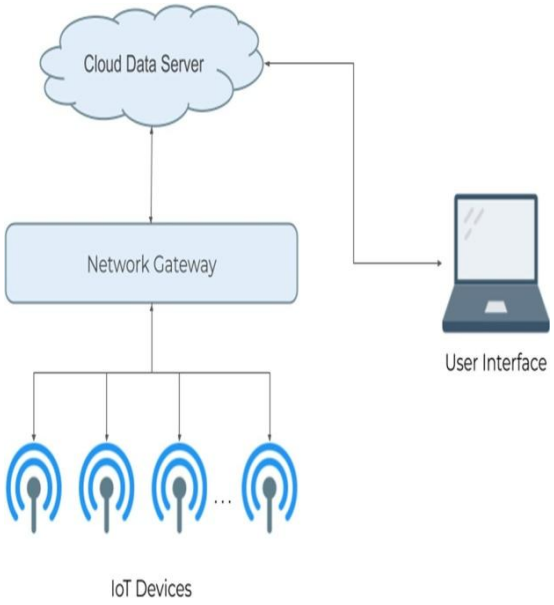

Figure 4: The Interface of IoT Devices

A. Initial Reconnaissance

IoT attackers often scan devices to identify vulnerabilities before attempting a cyberattack on an IoT device. This is often done by purchasing a copy of the IoT device you are targeting on the market. Then they develop it . A device for creating test attacks to see what output can be obtained and what is the potential for attacking the device. Examples of this include opening the device or analyzing internal hardware such as flash memory to do this. Learn about software and operate microcontrollers to identify or unintentionally trigger sensitive information Action.

To counter reverse engineering, it is important that IoT devices have hardware-based security. The application processor, which consists of sensors, actuators, power supplies and connections, should be housed in one Tamper-proof environment. Device authentication can also be performed with hardware-based security, so the device can prove to the server to which it is connected that it is not fake.

B. Physical Attacks

Low-tech category attacks often include physical attacks that use the hardware of the target device. In a way that benefits the attacker. There are different types of physical attacks. This includes attacks such as: As a fault attack, the network to which the device is connected is shut down due to interruption of function. Physically Damage damaged to prevent the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

device or its components from functioning properly. Malicious code injection. An example of this is when an attacker inserts a USB stick containing a virus into a target device.

Signal jammers are used to block or manipulate the signals emitted by the device. Constant denial. The service (PDoS) attacks described later in this white paper can be performed as physical attacks. For IoT devices for example, connecting to a high voltage source can overload its power system must be replaced.

C. Man-in-the-Middle

One of the most common attacks on the IoT is the Man-in-the-Middle (MITM) attack. For computers in general MITM attacks intercept communication between two nodes and allow an attacker to assume the role of proxy. Attacker Computer and router, two mobile phones.

Most commonly servers and clients. Figure 2 shows a simple example of a MITM attack between a client and a server. With respect to IoT, attackers typically perform MITM attacks between the IoT device and the application to which it is connected. Interface. IoT devices in particular tend to be more vulnerable to MITM attacks because there is no standard implementation to mitigate the attack. There are two common types of MITM attacks: cloud polling and direct connection. In the cloud

By polling, the smart home device keeps communicating with the cloud, mainly checking for firmware updates. An attacker can redirect network traffic by using ARP resolution protocol (ARP) poisoning or by modifying the Domain Name System. Set up or intercept HTTPS traffic using tools such as self-signed certificates or Secure Sockets Layer (SSL) strips Many IoT devices do not verify the authenticity or trust level of the certificate and do not create a self-signed certificate. A particularly effective method. For a direct connection, the device communicates with the hub or application

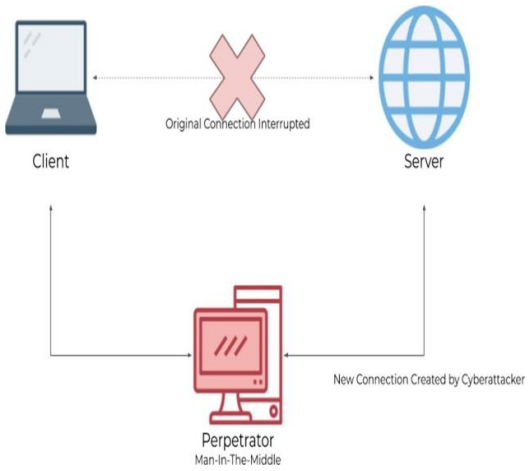

Figure 5: Connection between Client and Server

This allows mobile apps to find new devices by probing all IP addresses on the local network. Specific port. An attacker can do the same to discover devices on the network. An attack is a smart refrigerator attack that can display the user's Google calendar. Although it seems to be a harmless feature. The attacker discovered that the system did not validate the SSL certificate. This allows an attacker to carry out a MITM attack. Steal users' Google credentials.

D. Botnets

Another type of common attack on IoT devices is to recruit many devices to create botaked and start distributed rejection of service (DDOs) attacks. A refusal of the service attack (DOS) is characterized by an orchestrated end to prevent legitimate Use of a service.

A DDOS attack uses several business attacks to achieve this goal. DDOS attacks want overwhelming Infrastructure of the target service and disturb the normal dataflow. DDOS attacks generally go through a few phases: recruitment in which the attacker scans for susceptible machines to use the target against the attack of the DDOs and an infection in which the vulnerable machines are used, and the malignant code is injected.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

The attacker evaluates the infected machines that are online and decides when to schedule attacks, or upgrading the and attack in which the attacker commands the infected machines to send harmful packages to the destination

One of the most popular ways to obtain infected machines and perform DDOS attacks is due to IoT devices due to IoT devices their high availability and generally poor safety and maintenance. Figure 4 shows a typical command structure. The attacker's master computer sends commands to one or more infected command and control centers. Each can control a set of zombie devices and attack the target. One of the most well-known malware, the Mirai worm, has been used to carry out some of the biggest DDoS attacks to date.

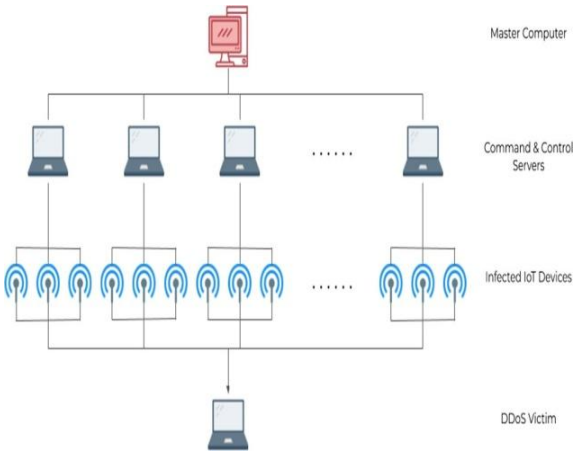

Figure 6: The DDOS Attack.

It is known and designed to infect and control IoT devices such as DVRs, CCTV cameras and home routers. Infected person .The device becomes part of a large botnet and can carry out different types of DDoS attacks. Mirai was made to handle it Several different CPU architectures commonly used in IoT devices such as B. x86, ARM, Sparc, PowerPC, Motorola, Record as many devices as possible, etc.

To keep it secret, the virus is very small and actually. Not on the device's hard drive. This remains in memory. That is, the virus will be lost after the device reboots. However, once infected, the device is vulnerable to reinfection because it has already been detected as such. It is vulnerable and can only be re-infected in a few minutes. Today, many well-known IoT botnets are targeting it. The virus originates from Mirai source code such as Okiru, Satori, Reaper, etc.

VIII. CONCLUSION

The IoT can best be described as an ever-evolving Complex Adaptive System (CAS). Therefore, evolution and management over the years requires new and innovative formats in software engineering, systems engineering, project management, and many others. The areas of application of IoT are very diverse in order to be able to serve different users with different needs. The fact that the IoT is so widespread that it affects almost every area of our lives has become an important research topic for research in various related areas such as information technology and computer science.

This white paper explores common strategies for disrupting or compromised the IoT and explains at the ground level how these attacks are carried out. If necessary, examples are also provided to clarify these explanations. Next, a number of AI algorithms are presented and their programs in cybersecurity are considered. Often, these epidemics are not uncommon in business programs, but are still rare, either researching or improving current processes, or still difficult to implement. Nonetheless, the mode mentioned is promising and is unlikely to become an unusual structure for attack detection within just a few years. The context of the IoT structure also describes how to attack and use AI to attack. With the boom in IoT structures, these types of attacks are becoming more and more threatening. In particular, it will be as a huge network begins experimenting with smart cities. Large networks with different attack surfaces are difficult to shield, and everyday life and protection revolve around AI, which is more or less resilient.

With the incessant burgeoning of the emerging IoT technologies, the concept of Internet of Things will soon be inexorably developing on a very large scale. This emerging paradigm of networking will influence every part of our lives ranging from the automated houses to smart health and environment monitoring by embedding intelligence into the objects around us. In

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

this paper we discussed the vision of IoT and presented a well defined architecture for its deployment. Then we highlighted various enabling technologies and few of the related security threats.

REFERENCES

[1]. M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)", in 2015 Internet Technologies and Applications (ITA), pp. 219– 224, Sep. 2015, DOI: 10.1109/ITechA.2015.7317398.

[2]. P. J. Ryan and R. B. Watson, "Research Challenges for the Internet of Things: What Role Can OR Play?," Systems, vol. 5, no. 1, pp. 1–34, 2017.

[3]. M. Miraz, M. Ali, P. Excell, and R. Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", Future Internet, vol. 10, no. 8, p. 68, 2018, DOI: 10.3390/fi10080068.

[4]. E. Borgia, D. G. Gomes, B. Lagesse, R. Lea, and D. Puccinelli, "Special issue on" Internet of Things: Research challenges and Solutions".," Computer Communications, vol. 89, no. 90, pp. 1–4, 2016.

[5]. K. K. Patel, S. M. Patel, et al., "Internet of things IOT: definition, characteristics, architecture, enabling technologies, application future challenges," International journal of engineering science and computing, vol. 6, no. 5, pp. 6122–6131, 2016.

[6]. AbdelRahman H. Hussein "Internet of Things (IOT): Research Challenges and Future Applications", Department of Networks and Information Security Faculty of Information Technology / Al-Ahliyya Amman University International Journal of Advanced Computer Science and Applications, Vol. 10, No. 6, 2019

[7]. Murat Kuzlu, Corinne Fair, Ozgur Guler "Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity" Discover Internet of Things (2021) 1:7 11-2020

[8]. M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal, "A Review on Internet of Things" March 2015 International Journal of Computer Applications 113(1):1-7