# Vulnerabilities, Threats and Challenges on Cyber Security and the Artificial Intelligence based Internet of Things: A Comprehensive Study

**Mohammed Ateeq Alanezi**

College of Computer Science and Engineering, University of Hafr Al Batin, KSA

**Abstract**
The Internet of Things (IoT) has gotten a lot of research attention in recent years. IoT is seen as the internet's future. IoT will play a critical role in the future, transforming our lifestyles, standards, and business methods. In the following years, the use of IoT in various applications is likely to rise. In the world of information technology, cyber security is critical. In today's world, protecting data has become one of the most difficult tasks. Different type of emerging cyber threats such as malicious, network based and abuse of network have been identified in the IoT. These can be done by virus, Phishing, Spam and insider abuse. This paper focuses on emerging threats, various challenges and vulnerabilities which are faced by the cyber security in the field of IoT and its applications. It focuses on the methods, ethics, and trends that are reshaping the cyber security landscape. This paper also focuses on an attempt to classify various types of threats, by analyzing and characterizing the intruders and attacks facing towards the IoT devices and its services.

***Keywords:***
*Internet of Things, Cyber security, Artificial intelligence (AI), Information technology, Networks, Malicious attacks.*

## 1. Introduction

Cyber security has been defined as "a body of technologies, practiced through an organized set of actions, meant to protect Networks, Computers, System Software Applications, and data from an attack, harm, or illegal access.". Malicious attacks, network attacks, and network misuse are all examples of Cyber Emerging Threats, according to experts. A malicious attack is any attempt to use another person's computer to corrupt the resources with viruses, Trojan horses, spyware, and other malware. Network attacks are acts that are intended to harm or disrupt the data flow of information in a Computer System on a Network Service account, resulting in effects such as Denial of Service (DoS) [1, 2], account hijacking, email fraud etc. Network misuse [3] is essentially an attack against a network's point of engagement, and it can be used in a variety of ways, including spam, phishing, and phishing emails. Cyber-attacks are usually seen as criminal acts carried out via the Internet. These exploits can include stealing an institution's intellectual property, capturing online bank accounts, developing and distributing Viruses on many computers, leaking confidential business information over the internet, and destroying a country's core public infrastructure. Internet threats are regarded as the most common cause of corporate failure and revenue losses across all organizations. [4]. "An effort to discredit or undermine the operation of a computer-based system, or an effort to track the online activities of individuals without their consent. Attacks of this nature may go undetected by the end user or cause the network to be completely disrupted, rendering none of the users unable to do even the most basic of operations" [5].

The Internet of Things has successfully brought the fictitious world and the actual world together on the same interface. The construction of a smart environment and self-aware autonomous devices, such as home automation, smart products, smart health, and intelligent buildings, are among the key aims of IoT [6]. The rate of adoption of IoT devices is currently very strong, with an increasing number of devices connected to the internet. Author in [7] estimates that there will be 30 billion linked things with around 200 billion connectivity by 2020, generating revenue of around 700 billion euros. In China, there are already nine billion gadgets, with the number predicted to rise to 24 billion by 2020. The Internet of Things will fundamentally alter our lifestyles and economic practices in the future. It will allow individuals and gadgets to connect at any time, from anywhere, with any device, in optimal circumstances, across any network and utilizing any services [8]. The major purpose of the Internet of Things is to build a better world for humans in the future. Figure 1 depicts the principle components of IoT architecture. It consists of cloud infrastructure, network infrastructure, things and the gateways. The cloud infrastructure comprises of the various devises that can access the complete hardware and the software components. It should also support the necessary requirements of a computing paradigm. The network infrastructure comprises of the various devises that can access the complete hardware and the software resources to enable the inter connectivity of resources in order to establish the secure connection between them [9]. It is also responsible for connectivity and communication establishments between the networks. The IoT gateways are responsible for establishing the communication in IoT.

Manuscript received February 5, 2022
Manuscript revised February 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.2.20

It can be usually device to device or peer to peer communication. It also acts as an administrator interface in between the peer to peer devices. Attackers and hackers target IoT devices on a daily basis. According to a survey, 70 percent of IoT devices are very easy to hack. As a result, an effective technique to protect devices connected to the internet from hackers and intruders is critical [10].

This paper seeks to contribute to a better understanding of emerging threats and the vulnerabilities of cyber security in the IoT and its applications which are originating from various intruders like organizations and intelligence. The process of identifying threats and vulnerabilities in the IoT based systems is necessary for specifying a robust, complete set of security requirements and also helps determine if the security solution is secure against malicious attacks in IoT based devices and its applications. The rest of the paper is organized as: Section 2 discusses motivation of the proposed work. While, Section 3 provides a brief overview about the cyber security, Emerging Cyber Security Threats, Section 4 depicts the discussion about Internet of Things, its devices, the security threats, Attacks, and Vulnerabilities in IoT. Section 5 depicts the conclusion of this comprehensive study.

## 2. Motivation of the proposed work

Challenges faced by the IoT based systems by Cyber security vulnerabilities are as follows:

- Various methods were proposed earlier for improving performance of Cyber security systems. Majority of the IoT systems are still in process for the enhancement of Cyber security and its threats and vulnerabilities, but with poor accuracy.
- Various methods were used earlier for improving the accuracy of cyber security in the IoT based systems. Though, it was highly scalable, but the performance was poor in terms of accuracy.
- As a result, detecting risks and vulnerabilities in AI and IoT based systems is required for defining a robust, comprehensive set of security criteria, as well as determining whether the security plan is secure against unwanted assaults.
- Application of Back Propagation Neural Networks detects the vulnerabilities more precisely.

## 3. Cyber Security:

Security is defined as a method for protecting an object from physical harm, illegal access, crime, or loss by maintaining high secrecy about the object and making that available information whenever it is required.
The technique of protecting computers, servers, mobile devices, communications devices, networks, and data from hostile intrusions is known as cyber-security. It's also known as electronic data security or information systems security. The phrase is used in a range of contexts, ranging from corporate to mobile computing, and it may be broken down into a few subcategories.

- Network security refers to the process of protecting a computer network from attackers, whether they are targeted attackers or reactive malware.
- Application security is concerned with preventing threats to software and devices. A hacked program could allow access to the data it was supposed to secure. Security starts throughout the design phase, long before a program or device is implemented.
- Integrity and privacy of data are secured by data security, both in storage and in transport.
- Procedures and choices for managing and safeguarding digital assets are included in security procedures. The protocols that dictate how and where data may be kept or exchanged, as well as the rights users have while connecting a network, all fall under this category.
- Disaster recovery and continuity planning are the terms that describe how a company reacts in the case of a cyber-security breach or any other catastrophe. This results in the loss of activities or data. Incident management policies define how an institution returns operations and data to the same operational capabilities as before the incident. Contingency planning is the plan that an organization uses when it is unable to operate due to a lack of assets.
- End-user training handles the most unpredictably and uncertain aspect of cyber-security. This can be done by failure to obey appropriate security measures. Anyone can unintentionally introduce a virus into an unprotected system [11]. It is critical for every organization to maintain the security by teaching users to delete suspicious email as attachments, not plug in unrecognized USB drives, and a variety of other key teachings etc.

### 3.1. Emerging Threats in Cyber Security

Every country on earth has a particular set of risks. In fact, any work of securing the web and staying ahead of

developing dangers can be a difficult one, even for PC users who are comfortable with security technologies . There isn't a week that goes by without a virus infection, an attempt of hacking, or a phishing scheme being reported. As a result, a variety of PC users, including those who have deployed security software such as firewalls, anti-virus, and specific filtering software, may be vulnerable to security risks [12] and software failures. These risks are usually classified as hostile, security breaches, or system abuse. Computer viruses, malware, Trojan, key loggers, and Automation tools are examples of malicious software. Ethical hacking, denial of service (DOS), phishing, and web deliberate destruction are all examples of network attacks. SPAM, phishing, and phishing emails are examples of network abuses, and some of these risks are discussed below in relation to network-related forgery cases [13]:

- Phishing and email Spamming
- Botnet
- Malware and Spyware
- Key loggers
- Social Engineering
- Denial of Service
- Virus
- Worm

## 4. Internet of Things

The Internet of Things (IoT) [14] is an extension of the Internet into the real world that allows users to interact with tangible objects in their environment. As shown in Figure 1, individuals, gadgets, and applications are fundamental notions in the IoT domain. Various projects have distinct definitions and distinct meanings for them.

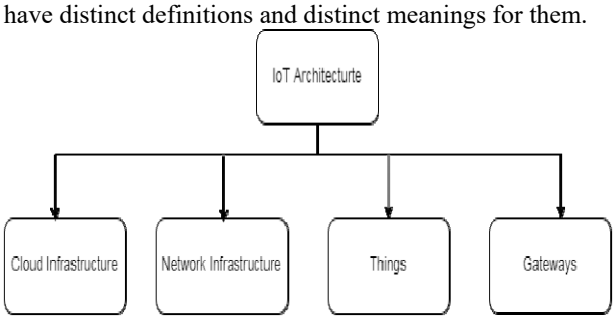


**Figure 1. Principle concepts of an IoT domain**

### 4.1 Devices for IoT based on AI

Artificial intelligence (AI) is the capacity of a system or a machine controlled by a computer to do normally require human cognition and discernment. AI also refers to the intelligence exhibited by machines rather than innate ability produced by animals such as humans. AI based IoT is a piece of hardware that enables the entity to interact the Back propagation Neural Network (BPNN), an AI based technology with the virtual environment [14]. It's also known as a sensible thing, which can be something really networked and equipped with sensors that provide information about the physical surroundings (e.g., temperature, moisture, existence detection systems, and emissions), sensors (e.g., lighting control, displays, motor-assisted shutters, or any other activity that a device can undertake), and embedded computers [15, 16]. A gadget that is part of the Internet of Things can communicate with other IoT devices and ICT systems. Cellular (3G or LTE), WLAN, wireless, and other technologies are used to connect between these devices [8]. The size, i.e., tiny or ordinary; portability, i.e., portable or fixed; indoor or outdoor source of power; if they are attached infrequently or always-on; done by robots or non-automated; physical or logical entities; and, finally, if they are IP-enabled entities or non-IP devices determine IoT device classification. The ability to automate and/or detect, the ability to limit power/energy, connectivity to the physical environment, inconsistent connection, and portability are all properties of IoT devices. Others may not need to be fast and dependable, or provide convincing security and privacy [9]. Some of these gadgets are protected physically, while others are left unsupervised. In reality, devices in IoT contexts should be safeguarded from any risks that could compromise their operation. However, because of their features, most IoT devices are susceptible to both external and internal assaults [16]. Due to resource limits in terms of IoT processing capabilities, storage, and battery capacity, implementing and using an effective security mechanism is difficult.

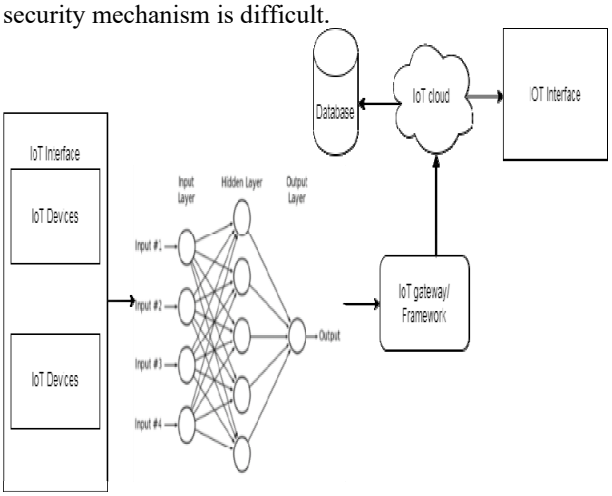


**Figure 2: The concept of IoT and AI**

## 4.2. Security Threats, Attacks, and Vulnerabilities in IoT

The resources available (system components) that constitute the IoT must first be recognized before security concerns which can be addressed. Understanding the asset management system, which includes all IoT modules, devices, and applications, is critical. An asset is a valuable and sensitive economic asset that belongs to a company. The system hardware (which includes buildings, machines, and other items), firmware, applications, and data provided by the services are the most important assets of any Iot environment.

### 4.2.1 Vulnerability

Security flaws are defects in a system's architecture or functionality that allow an attacker to run commands, access information without permission, and/or launch DOS attacks. In IoT systems, weaknesses can be found in a variety of places. They can include flaws in systems hardware or software, as well as flaws in system policies and processes. it also includes the flaws in the network users themselves [7]. IoT systems are made up of two basic components such as system hardware and system software in which, both of which are prone to design faults. Hardware attacks are hard to find and repair, even when they are found, due to hardware compatibility and interoperability, as well as the time and effort required to fix them. Operating systems, application software, and control software, such as communication systems and device drivers, all have software attacks. Program design faults are caused by a variety of variables, particularly human factors and software complexity. Human flaws are frequently the source of technical attacks. Creating the project without a plan, inadequate communication between developers and users, an insufficient resources, abilities, expertise, and failing to manage and control the system are all examples of not knowing the needs [7].

### 4.2.2 Exposure

An attacker can execute intelligence gathering activities due to a flaw or mistake in the system configuration. Adaptive capacity against physical threats is one of the most difficult concerns in the IoT. In most IoT applications, devices are likely to be left unsupervised and positioned in areas that are readily available to attackers. As a result of this vulnerability, an attacker may be able to capture the device, extract cryptographic credentials, modify its code, or replace it with a hostile device under the attacker's control.

### 4.2.3 Threats

A threat is an event that exploits a system's security flaws to cause harm to it. Humans and environment can both pose threats. Extreme events, storms, cyclones, and fires have the potential to destroy computer systems. Natural disasters are difficult to prevent, and few safeguards can be put in place. The greatest techniques to secure systems from natural risks [11] are disaster response strategies, such as backup and contingency plans. Human threats are those that are created by people, such as malicious threats that are either internal (somebody has permitted access) or exterior (participants or groups acting outside the network) in nature and seek to harm or damage a system. The following types of human dangers are classified:

- Structured threats: people who are aware of system threats and can understand, develop, and exploit codes and scripts;
- Structured threats: people who are aware of system threats and can recognize, create, and utilize codes and scripts;
- Advanced Persistent Threats (APT) is an example of an organized threat. APT is a complicated network assault that aims to steal data from high-value data in business and government entities such as industrial, finance, and domestic security.

As the IoT becomes a fact, the number of security risks has increased, posing a risk to the general public. Unfortunately, the Internet of Things brings with it a new set of security risks. There is a growing understanding of cyber security and the IoT as a rising awareness that the new generation of smartphones, laptops, and other gadgets may be exploited by malware and thus subject to attack.

### 4.2.4 Attacks

Vulnerability are attempts to destroy a system or interrupt regular operations by utilizing various strategies and tools to find weaknesses. Intruders carry out attacks for a variety of reasons, including personal gratification or monetary gain. The word "attack cost" refers to the assesement of an attacker's challenges in terms of their skill, assets, and purpose. People who pose a threat to the digital realm are known as attack agents [6]. Hackers, criminals, or even governments could be involved [7]. Section 3 delves more into the subject. Active cyberattacks, such as monitoring un-encrypted traffic in search of confidential material; passive attacks, such as tracking undefended network communications to decipher loosely encoded traffic and obtain user credentials; close-in

attacks; insider exploitation, and so on, are all examples of attacks [21-25]. The following are examples of common cyber-attacks

(a) Physical attacks
The hardware devices are tampered with in this type of assault [20]. Most IoT devices operate in outdoor locations, which are especially vulnerable to physical attacks due to their unsupervised and scattered nature.

(b) Intelligence based attacks
Intelligence gathering attacks include the illegal discovery and identification of systems, resources, or attacks. Monitoring the network access points, packet packet sniffing, network monitoring, and making queries regarding IP address details are all examples of Intelligence gathering based attacks.

(c) Denial-of-service (DoS):
An effort is made to make a system or network device inaccessible in this type of attack [19]. The bulk of IoT devices are susceptible to resource enervation attacks due to their poor memory capacities and restricted computing resources.

(d) Access attacks
Unauthorized individuals obtain access to networks or systems to which they do not have permission. There are two sorts of accessibility attacks:

1. Access control, in which an attacker gains physical access to a device.
2. Remote control to IP-connected systems.
3.

(e) Attacks on privacy
Since, enormous amounts of data are easily accessible through remote access techniques [18], information privacy in the IoT has become increasingly difficult. The following are the most prevalent attacks on privacy protection:

- Data mining: allows attackers to find the data in databases that they weren't expecting.
- Cyber espionage: obtaining secret data from users, companies, or the government by utilizing breaching techniques and harmful software.
- Eavesdropping is the practice of monitoring in on a discussion between two people.
- The computer's unique identifying number can be used to trace a user's activities. Tracking the location of a user makes it easier to identify them in instances where they don't want to be identified.

(f) Password-based attacks
Intruders are attempting to replicate the password of a valid user. This attempt can be carried out in two ways:
1) Dictionary based attack - attempting to guess user passwords using variety of letters and digits
2) Brute-force assaults, which involve employing breaching tools to try all feasible password sequences in order to find legitimate passwords.

(g) Cyber-crimes
Users and data are exploited through the Internet and smart things for monetary benefit, such as online piracy, identity fraud, trademark theft, and fraud [6, 7, 17].

(h) Destructive attacks
Space is being exploited to interrupt and destroy people and assets on a large scale. Terrorism and retaliatory attacks are examples of harmful attacks. g) Data Acquisition and Supervisory Control (SCADA) Attacks: The SCADA system, like any other TCP/IP system is subject to a variety of cyber-attacks . Any of the following methods can be used to attack the system:
i. Using DoS attacks to bring the system to a halt.
ii. Taking control of the system with Trojans or malware.

## 5. Conclusion and Future Enhancements

The goal of this study is to assess the categorization of various system underlying hazards. This expose IoT architecture and applications to various cyber threat vectors and make a case for research in this developing technology. The topic of our talk is the discovery of various attacks found in IoT application and service areas. On a configuration of smart metering infrastructure, the authors ran two different attack scenarios . The findings of our experiments reveal that multiple threat actors could leverage designed vectors to exploit susceptible IoT systems (whether it's an application, hardware, software, or firmware). Finally, it is vital to continue the conversation while also forcing device manufacturers and element suppliers to build and execute solutions to counteract cyber-threats in order to ensure customer confidence in IoT innovation and change.

## References

[1] A. Prakash, M. Satish, T. Sri Sai Bhargav, N. Bhalaji, Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture, Procedia Computer Science, Vol 87, 2016, pp. 275-280.

[2] Distributed Denialof-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms in Advance Computing Conference, 2009. IACC 2009. IEEE International (2009), pp. 1275-1280

[3] Jonathan D. Fuller, Benjamin W. Ramsey, Mason J. Rice, John M. Pecarina, Misuse-based detection of Z-Wave network attacks, Computers & Security, Vol 64, 2017, pp 44-58,

[4] Williams CM, Chaturvedi R, Chakravarthy K Cybersecurity Risks in a Pandemic J Med Internet Res 2020 vol. 22, no. 9, e23692 doi: 10.2196/23692

[5] Keskin, O.F.; Caramancion, K.M.; Tatar, I.; Raza, O.; Tatar, U. Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. Electronics 2021, 10, 1168. https://doi.org/10.3390/electronics10101168

[6] Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. 2018. The Industrial Internet of Things (IIoT): An Analysis Framework. Computers in Industry 101: 1–12.

[7] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[8] Lin, Shi-Wan, Brandford Miller, Jacques Durand, Graham Bleakley, Amine Chigani, Robert Martin, Brett Murphy, and Mark Crawford. 2019. The Industrial Internet of Things Volume G1: Reference Architecture V1.90. Industrial Internet Consortium, June. Accessed January 2022. https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[9] J. Fuller, B. Ramsey, Rogue Z-Wave Controllers: A Persistent Attack Channel, in: 10th IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp), 2015, pp. 734–741

[10] B. Ramsey, B. Mullins, Defensive Rekeying Strategies for Physical-Layer-Monitored Low-Rate Wireless Personal Area Networks, in: J. Butts, S. Shenoi (Eds.), Critical Infrastructure Protection VII, Vol. 417 of IFIP Advances in Information and Communication Technology, Springer Berlin Heidelberg, 2013, pp. 63–79

[11] Gritzalis, D.; Stergiopoulos, G.; Vasilellis, E.; Anagnostopoulou, A. Readiness Exercises: Are Risk Assessment Methodologies Ready for the Cloud. In Advances in Core Computer Science-Based Technologies; Springer: Cham, Switzerland, 2021.

[12] Desnitsky, V.; Kotenko, I. Modeling and Analysis of IoT Energy Resource Exhaustion Attacks. In Econometrics for Financial Applications; Springer Science and Business Media LLC: Berlin, Germany, 2017; Volume 737, pp. 263–270.

[13] Noshina Tariq, Farrukh Aslam Khan, Muhammad Asim, Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis, Procedia Computer Science, Vol 191, 2021, pp 425-430, https://doi.org/10.1016/j.procs.2021.07.053..

[14] M. Tariq, H. Majeed, M.O. Beg, F.A. Khan, A. Derhab Accurate detection of sitting posture activities in a secure iot based assisted living environment Future Generation Computer Systems, 92 (2019), pp. 745-757

[15] S. Shukla Reliable critical nodes detection for internet of things (iot) Wireless Networks, 27 (4) (2021), pp. 2931-2946

[16] G. M. Køien, "Reflections on trust in devices: an informal survey of human trust in an internet-of-things context," Wireless Personal Communications, vol. 61, no. 3, pp. 495–510, 2011.

[17] Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. SN Appl. Sci. 3, 121 (2021)

[18] Babaei A, Schiele G (2019) Physical unclonable functions in the Internet of Things: state of the art and open challenges. Sensors 19(14):3208

[19] Om Kumar CU, Bhama PRKS (2019) Detecting and confronting flash attacks from IoT botnets. J Supercomput 75(12):8312–8338

[20] Aldaej A (2019) Enhancing cyber security in modern Internet of things (IoT) using intrusion prevention algorithm for IoT (IPAI). IEEE Access. https://doi.org/10.1109/ACCESS.2019.2893445

[21] Alshehri MD, Hussain FK (2019) A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing 101(7):791–818

[22] Yuchong Li, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021, Pages 8176-8186

[23] Priyadarshini I., et al, Identifying cyber insecurities in trustworthy space and energy sector for smart grids, Comput. Electr. Eng., 93 (2021), Article 107204

[24] Ogbanufe O, Enhancing end-user roles in information security: Exploring the setting, situation, and identity, Comput Secur., 108 (2021), Article 102340.

[25] Niraja K.S., Srinivasa Rao S, A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security, Mater. Today: Proc. (2021