International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
***Article Received**: 18 October 2022 **Revised**: 24 November 2022 **Accepted**: 19 December 2022*

Security Awareness Model for Artificial Intelligence and Internet of Things

[1]Krishan Kant Singh Gautam, [2]Rajendra Kumar
[1]Department of Computer Science, Jamia Millia Islamia, A Central University
New Delhi, India.
gautamkrishankantsingh@gmail.com
dr.kksgautam@gmail.com

[2]Department of Computer Science, Jamia Millia Islamia, A Central University
New Delhi, India.
rkumar1@jmi.ac.in

Abstract—With human engagement replacing artificial intelligence in the provision of services, the position of intelligence systems is rapidly changing. The Internet of Things (IOT) plays a prominent role in these variations as it is a cutting-edge and developing technology that connects physical objects to the virtual world, enabling anytime, everywhere connectivity for anything. A technology known as the Internet of Things (IOT) enables the networked connection and data transfer of physical objects, people, gadgets, cars, and other things. IOT eliminates the need for computer-human contact by speaking directly to the user.This encourages increased communication between entities as a result. It can enhance the fundamental services provided in the industries of transportation, banking, healthcare, and education. Recent analyses have shown that the Internet of Things (IOT) and its related components are very susceptible to security vulnerabilities. Using artificial intelligence approaches, IOT security issues can be rectified (AI). AI develops crucial apps that enable data flow in an IoT environment. Intelligent transmission technique.

Keywords-Banking;Healthcare;Logistics;Intelligence Systems

I. Introduction

IOT is probably going to speed the spread of internet-connected services in the future years. In 1999, British technology pioneer Kevin Ashton coined the term "IOT." IOT is a system that enables physical objects to be connected to the Internet via sensors, according to Kevin's definition. Smart cities, smart retail, smart phones, environmental monitoring, and healthcare are just a few of the many applications for IOT.

Figure 1 shows the historical and projected service needs per person, which are expected to rise sharply in the near future, according to a 2011 Cisco estimate. We will take this need into account based on the end user devices that are connected to the network [1, 11]. It illustrates the current and upcoming developments in personal technology. Figure 1 shows a distinct pattern. The requirement for IOT infrastructure security management is expanding swiftly, yet the number of devices is not keeping up. [2].

In today's digital environment, where it is now hard to ignore, we are all aware of how important security is. Later in this essay, the bulk of security issues surrounding IOT services—whether they are advantages, interests, or social acceptance—are discussed in more detail. One of the main issues with IOT services is the security of the "route of delivery" to end users. This is explained in this work using a layered model [3]. There are several ways to solve these problems, but in this work, we provide an AI perspective to deal with them in a modern manner.

In many computing fields, especially security, where it is necessary to choose which service parameters must be controlled and to what extent in order to safeguard the system with intelligence, AI is advantageous because it starts the process by which a machine's decisions start to resemble those of a human. Integration of IOT and AI is essential for security as it strengthens the IOT infrastructure. [4].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
***Article Received**: 18 October 2022 **Revised**: 24 November 2022 **Accepted**: 19 December 2022*

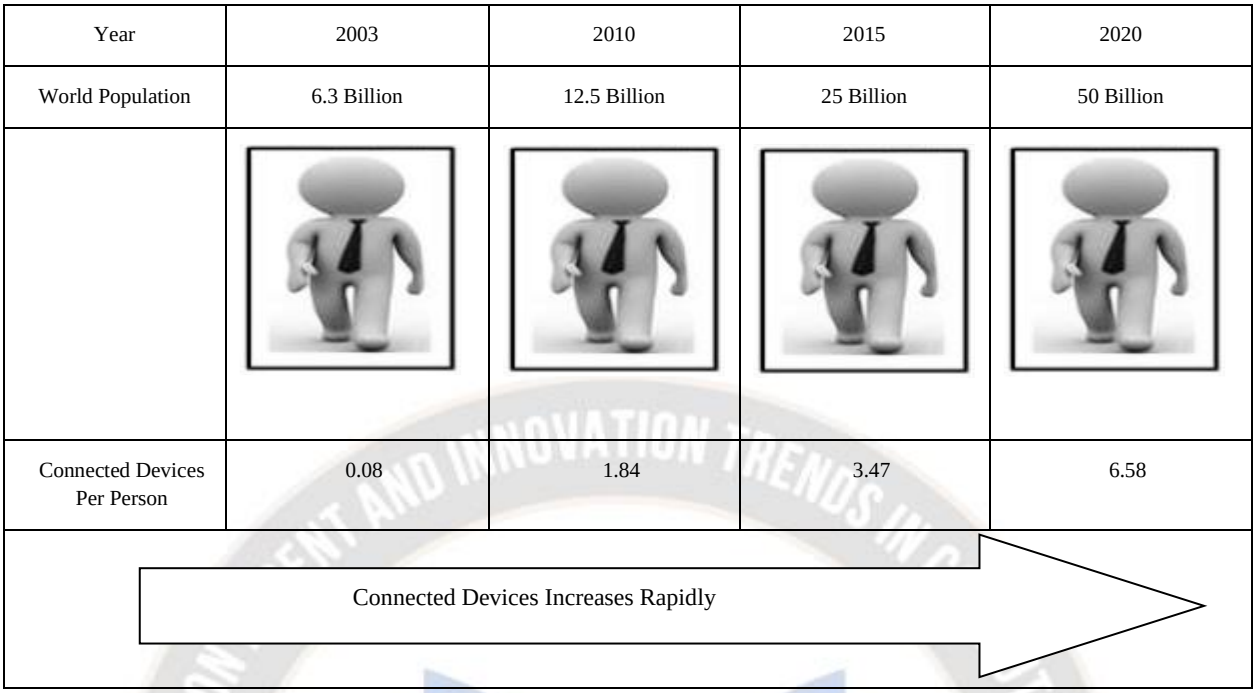

Figure 1. Number of Connected Devices per Person Trend

A. Security Needs in IoT

- *IoT Security and Privacy are Critical*

Since many different types of connected devices share data, just like in the Internet of Things, data privacy and information security are essential (IOT). For instance, the hacker has access to the user's trip itinerary data. Information security is thought to secure information's integrity, confidentiality, and accessibility [5].The risk of numerous online attacks and physical harm is increased by the IOT Security System, a network of small devices connected to business networks that collect or store a lot of user data and provide services to IOT users. The IOT Security system is made up of several items or gadgets that exchange a lot of data and need to be secure and private. Information security and privacy in IOT are difficult, nevertheless, due to the large variety of devices, things, and data. [6]. Table 1 below provides a summary of further implications.

TABLE – IGENERAL SECURITY THREATS IN IOT

S. No.	Threats	Details
1	Firmware/Software	Software and firmware are located in remote areas, making it simple to alter or attack them. Attacker may disregard the denial of a facility attack in order to hack the data.
2	Communication	Different devices can share data with one another simultaneously in an IOT network. Therefore, there is a high potential for many types of attacks, such as man-in-the-middle, eavesdropping, and traffic rerouting.
3	Physical insecurity	In the Internet of Goods, things or devices are positioned remotely, so there is no physical control, such as soil sensors in agriculture.
4	Highly mesh network	There are increased chances of an assault because the Internet of Things is such a tightly knit network of objects or gadgets.
5	Classic web threats	As all items or devices in an IOT network are connected, there are greater chances for an attacker to use techniques like XSS, CSRF, etc. to attack.
6	Cost	Because they are exclusive, it is difficult to purchase sensors with encryption coprocessors.

- Considered IOT Security Solutions

Every layer and pillar of the IOT Security system must be secure. Figure-2 shows pillars that illustrate the impact of potential security openings at each pillar [7].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
***Article Received**: 18 October 2022 **Revised**: 24 November 2022 **Accepted**: 19 December 2022*

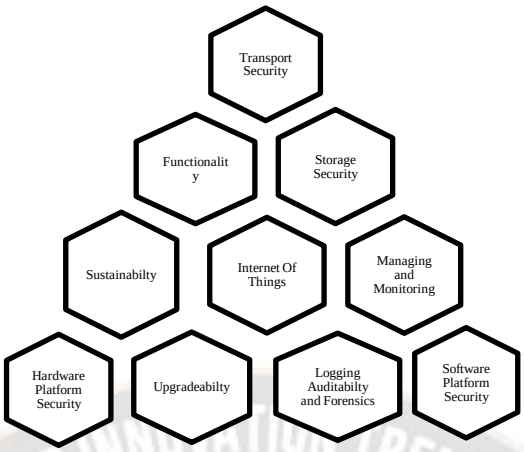

Figure 2. Pillars of IOT Security System

The IOT is expanding connections between people and things and producing quantities of data that were previously unimaginable. Table 2 describes each security pillar's function in detail.

TABLE – II SECURITY PILLARS OF IOT.

S. No.	Pillar	Details
1	Transport Security	For the Internet of Things to provide privacy and dependability for network communication, transport security must be carefully considered.
2	Storage Security	Tenacious data saved on devices is protected by storage security.
3	Software Platform Security and Execution	Selection and application platforms that give a stable environment, including software platforms, must be made even safer for IOT security systems.
4	Supervision and Monitoring	Verifying the management and monitoring of IOT devices in a secure manner.
5	Logging, Auditability and Forensics Enablement	Audit logs need to be protected. Data can be intercepted by the attacker by abusing the audit logs.
6	Sustainability and Upgradeability	Topographies that make it easier to upgrade devices securely after problems must exist.
7	Hardware Platform Security	Check to see if the hardware podium has the necessary security measures.
8	Functionality Security	Ensure security at a purposeful level that is steadfastly focused on the user interface of the programme.

B. AI Techniques to Resolve Issues of Security in IoT

John McCarthy, the "father of AI," defined artificial intelligence as "the science and engineering of developing intelligent machines, notably clever computer programmes." Robots can make good decisions in a way that is similar to how highly intelligent people think thanks to artificial intelligence. Understanding how the human brain works and how individuals learn, make decisions, and collaborate to solve issues is crucial for developing intelligent software and systems [16]. In essence, it creates an expert system with machine intelligence built in, resulting in a system that understands, thinks, learns, and behaves like a person. In order to reduce security concerns as mentioned earlier in the previous sections, we have recommended using AI approaches for IOT systems. Few AI techniques are as extensive as those in Table 3 with their advantages and disadvantages for reducing IOT security concerns [8–11].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
***Article Received**: 18 October 2022 **Revised**: 24 November 2022 **Accepted**: 19 December 2022*

TABLE – 3ADVANTAGES AND DISADVANTAGES OF VARIOUS AI TECHNIQUES

S. No.	Artificial Intelligence Technique	Advantage	Disadvantage
1	Neural networks	It provides a straightforward model that can be further modified to apply difficult real-world scenarios.	The networking topology is too intricate for practical usage.
2	Decision support system	In order to make significant, group decisions, a pool of data is also examined using data mining techniques	Private information that is frequently the target of system security attackers is also included in the user's data.
3	Expert systems	Give practical solutions to problems in the areas of medicine, communication, etc. by employing specialized tools and methods.	One error at the initial phases of implementation could lead to exponentially more errors afterwards.
4	Fuzzy logic	Boolean logic comes to rest where works.	They may or may not set the new environment's rules.
5	Image processing	In general, it is beneficial in industries that take into account human interfaces. The photographs are separated and compressed for various reasons.	A significant initial investment is required to purchase image processing equipment.
6	Information retrieval and pattern recognition	We look at information retrieval models and come up with a number of well-known patterns.	The results might or might not be highly reliable.

II. Purpose of Study

The Secure Internet of Things Project is a multidisciplinary research initiative that includes the Universities of Michigan, Stanford, and California-Berkeley. The focus of the research is on three main areas:

A. Hardware and Software Systems

Development of the intellectual property (IP)-protected hardware and software systems that enable IoT enabled systems.

B. Analytics

Integrating and examining the vast streams of instrumentation from the physical world along with all of the current data.

C. Security

Technological innovations in universal sensing and investigation to maintain and safeguard user security

III. Proposed Methodology

For this research, it is advised to combine quantitative and qualitative data collection methods. The ubiquity of misunderstandings makes quantitative methods of data collection more practical. Participant observation, interviews, and reflection are more suited when more in-depth data is needed, like in the case of attitudes toward using the CAI package.

A. Data Analysis

The data will be scrutinized using mathematical programmes, the interviews will be recorded, and the results will be coded.

B. Limitations and delimitations

One issue with the study is the validity of generalizations given the use of a specific topic. The novelty effect and pictures may also help people recall the material.

In order to proactively defend against and mitigate intrusions that are identified by the intrusion detection system's detection methods, Internet of Things (IoT) devices are the systems that are utilised as add-ons to IDS. The report that the IDS generates after reviewing the forensic analysis's report serves as the foundation for the suggested method.

The main assumption of this study is that an existing, adaptable Internet of things IDS already exists [12]. The usage of analysed forensic log data and appropriate report output forms the basis of a customizable IoT intrusion detection system. Two types of nodes are presumpted in the proposed IPAM (intrusion Prevention Algorithm in IoT): standard IoT nodes and intrusion detection nodes, which take advantage of the existing IoT infrastructure to create management networks. After a predetermined threshold hold period, all of the selected IDS nodes transfer the data packets they have collected to the main IDS station in charge of keeping track of network activity.

Following the completion of this procedure, the data from the merged log files is altered using forensic analysis, and a report is generated. Data elements like packet size, packet type, node ID, event type, routing protocol specifics, and time stamps are all included in these packet-level log files. The forensic analysis programme uses an elimination strategy and retrieves results as IDS repetitions using a variety of subsequent log search strategies. I thus attempted to improve the functionality of these already-existing IDS

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
***Article Received**: 18 October 2022 **Revised**: 24 November 2022 **Accepted**: 19 December 2022*

models based on them and created a DDoS attack avoidance strategy. Figure 3 [13] shows the security system.

The study includes an IDS analysis schema, which might only serve as an example of how network security will be evaluated generally at some point in the future. It is simple to create an APD if the frequency and behaviour of the attacker nodes have been statistically evaluated (Active Profile Database). Aset "R" that records the list of malicious nodes that have been identified and the assaults they have launched. This set then provides details on attacks, including the type of attack, the category of interaction (Active-Passive), and the list of attackers that have been identified.

For a longer time, this active profile database can offer a statistical study of the traits of each malicious node. These findings increase the likelihood that crucial information will be discovered to prevent such assaults in the future.

Each network node is iteratively screened with the IDS module's report included. The extent of the assault and the evidence of malicious nodes can be organized, and a report will be generated after each IDS cycle. If the current value of a malicious node is modified, the update scheme for the active profile database will be initiated, provided that the malicious node has been identified. Offering an adaptable and iterative security system that is aware of all the most recent updates is one of the main goals of our suggested method. This feature causes the offered solution to include a blacklist table, which is a neat list of nodes ordered according to how harmful they are.

Figure 3 illustrates the preclusion system's suggested algorithm and flowchart. The preventative threshold, which represents the highest number after which a malicious node will be banned [13], is an assumed integer denoted by the symbol.

R is a representation of the group of nodes that the Intrusion Detection System's most recent iteration determined to be hazardous. Each R component has a corresponding node ID, which acts as a distinctive identifier and is used in later studies. The fictitious network includes N nodes, and each node's malicious status number, denoted by S, is tracked by APD. As a result, the active profile database updates the node's Si number whenever a node with ID I is discovered to contain dangerous characters; otherwise, the table will maintain its current value of Si.

The node IDs will be added as a new item to the table of black flagged IDs' represented as "B" if the Si number is greater than the threshold number set in "p" in that circumstance. The reactive module will get feedback from the planned preventative procedure about what needs to be done by the system to protect and maintain the network's security and performance. Nodes in blacklist tables (value>p) are thought to have a higher likelihood of being malicious.

The system's response architecture will restrict the functioning of these selected nodes, classify them as unreliable, and isolate them from building any portion of the network route as a preventative step. These nodes may even be labelled as incompetent and altogether cut off from the network in very extreme cases. The likelihood of learning about some nodes' actions is included in the intrusion detection system's report, so these nodes are placed to the blacklist table, where their functionality and behaviours are recorded and evaluated both individually and collectively.

The reaction technique will include schematic functions that are dependent on one another and used in specific attack occurrence scenarios. Based on the information response that the preventative scheme detects, several functions are performed. The improvement, or at least maintenance, of the IoT network's performance in the event of an assault is one of the objectives of the suggested architecture. The reaction module will be activated if the blacklist table is modified, and the most serious prevention advice would be to isolate the afflicted devices from any network activity [13].

Where Ts is the length of time for the simulated network activity (10 continuous same intervals of time). To finish the IDS analysis, six consecutive forensic investigation iterations were performed, and everyone contributed an explicit and precise list of suspect nodes that ultimately resulted in the development of set R. The complete scheme can be put into action throughout a lengthy simulation period or during certain time slots that can validate the number of attacks or the presence of attackers [13].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
Article Received: 18 October 2022 Revised: 24 November 2022 Accepted: 19 December 2022

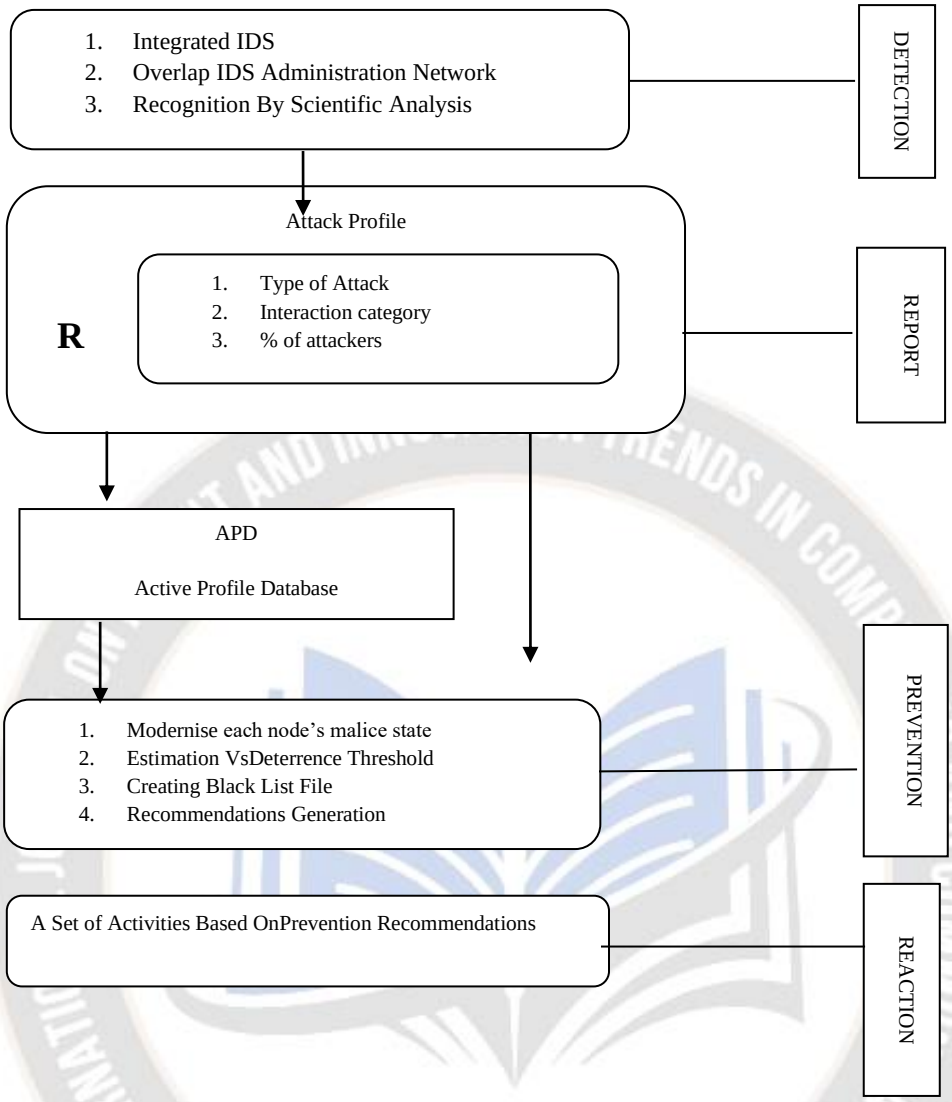

Figure 3. Proposed Security System Overview [13]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
Article Received: 18 October 2022 Revised: 24 November 2022 Accepted: 19 December 2022

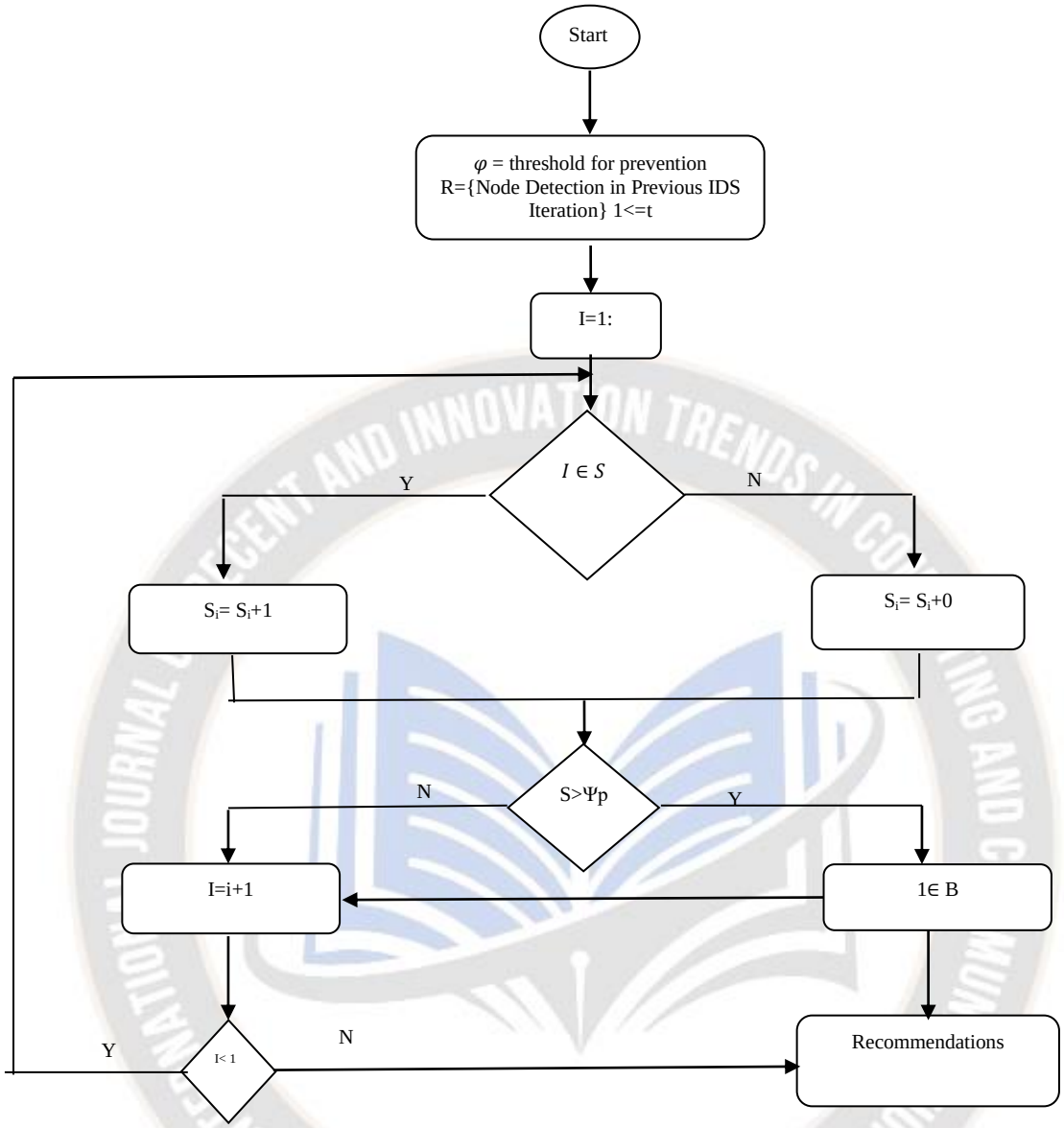

Figure 4.Intrusion Prevention Algorithm for IoT (IPAM) Algorithm Chart [13]

IV. Conclusion and Future Scope

Due to the IOT's youth and rapid expansion, there are numerous security and privacy problems. As a result, we discussed the IOT's privacy and security concerns. Researchers must consider a lot of challenges because the IOT Security system comprises of so many unique devices and parts. Due to the massive amounts of data that network devices in the IOT exchange, there are more chances for data breaches and data storage is particularly difficult, both of which need to be taken into mind. IOT security technologies pose significant privacy and security challenges. IOT are excellent platforms for implementing AI. Digital services may become fully automated as IOT service networks get bigger and more people use them. With the aid of AI techniques, the main privacy issues and their solutions could be highlighted. Due to its ability to learn and develop, artificial intelligence (AI) techniques for IOT security are currently receiving the most attention. This is because they are more precise and successful at thwarting the great majority of unanticipated attacks. The creation of a new security and privacy architecture is required for future solutions that make use of existing and emerging technology.

The intensity of DDoS and the ensuing damage have increased with the advent of several diversified attack sources, creating an environment that is favorable to harming the security and functionality of IoT technology. Attack frequency and impact might hinder genuine users from using the network's services and further deteriorate network performance. This paper focuses on potential security measures and proposes an IoT network-appropriate DDoS attack avoidance method. Based on the basic

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
DOI: https://doi.org/10.17762/ijritcc.v10i12.5936
***Article Received**: 18 October 2022 **Revised**: 24 November 2022 **Accepted**: 19 December 2022*

structure and workings of the present IDS. You can then suggest ideas for reaction modules and take action to guarantee network functionality, safety, and survival in the case of an attack.

REFERENCES

[1]. J.Gubbi, R.Buvya, S. Marusic and M. Palaniswami, "Internet of things: A vision, architectural elements, and future directions," in Elsevier, 2013, pp. 1645-1660.
[2]. Kopetz, H. (2011). Internet of things. In Real-time systems (pp. 307-323). Springer US.
[3]. Weber, R. H., & Weber, R. (2010). Internet of Things (Vol. 12). New York, NY, USA: Springer.
[4]. Wortmann, F., &Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57(3), 221-224.
[5]. A. W. Burange and H. D. Misalkar, "Review of inernet of things in development of smart cities with data management and privacy," in international conference on advances in computer engineering and application, IEEE,2015, pp. 189-195.
[6]. K. Zhao and L. Ge, "A survey on the internet of things security," in IEEE, 2013, pp. 663-667.
[7]. C. W. Axlrod, "Enforcing security, safety and privacy for the internet of things," in systems, applications and technology conference (LISAT), IEEE, 2015.
[8]. Sattikar, A. A., & Kulkarni, R. V. A Role of Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking.
[9]. Poniszewska-Maranda, A., & Kaczmarek, D. (2015, September). Selected methods of artificial intelligence for Internet of Things conception. InComputer Science and Information Systems (FedCSIS), 2015 Federated Conference on (pp. 1343-1348). IEEE.
[10]. Chakrabarti, P. (2009). Information Security: An Artificial Intelligence And Data Mining Based Approach. International Journal of Engineering and Technology, 1(5), 448.
[11]. Sumit Kumar, Zahid Raza, "Internet of Things: Possibilities and Challenges", International Journal of Systems and Service-Oriented Engineering (IJSSOE), IGI Global, pp 32-52 Volume 7, Issues 3, July-September 2017, ISSN 1947-3052, DOI: 10.4018/IJSSOE.2017070103.
[12]. Sharma, P., Sharma, N., & Singh, R. (2012). A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network. International Journal of Computer Applications, 4121, 975–8887. doi:10.5120/5824-8064.
[13]. AbdulazizAldaej"Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)" IEEE Access, VOLUME XX, 2017, DOI 10.1109/ACCESS.2019.2893445.
[14]. A. V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," IEEE, vol. 49, no. 8, pp. 112–116, Aug. 2016.