International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2390388

IntelliGuard: Protecting IoT from AI-driven Cyber Attacks

Mrs. Rashmi Pandey, Ayush Sharma, Devansh Kulshrestha, Devraj Singh Tomar, Dhwaj Sharma
Department of Computer Science, ITM Gwalior, Madhya Pradesh, India

ARTICLEINFO

Article History:

Accepted: 01 June 2023
Published: 07 June 2023

Publication Issue
Volume 9, Issue 3
May-June-2023

Page Number
389-397

ABSTRACT

AI is the science and engineering concerned with the computational understanding of intelligent behaviour and the creation of intelligent machines.

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

This paper explores the relationship between Artificial Intelligence (AI) and the Internet of Things (IoT), and the role of AI in securing IoT devices. The paper defines AI as the science of creating intelligent machines that can perform tasks that require human intelligence, while IoT is a network of physical objects embedded with sensors, software, and other technologies that can communicate and exchange data with other devices and systems over the internet. The paper discusses how AI can extract meaningful patterns from the data generated by IoT devices and make decisions based on that data, leading to new and innovative solutions that can improve people's lives and transform industries. The paper also emphasizes the vulnerability of IoT devices to cyberattacks and highlights the importance of AI approaches, such as machine learning, support vec0tor machines, and neural networks, in identifying threats and potential attacks. Overall, this paper concludes that AI plays a crucial role in securing IoT devices and enabling the IoT to reach its full potential.

Keywords : Internet of things, IOT, Artificial Intelligence, Cyber Attacks, Security

I. INTRODUCTION

A. What is IoT?

The community of bodily items—"matters"—which might be incorporated with sensors, software, and other technology for the reason of speaking and sharing information with other devices and structures over the internet is typically mentioned by using the acronym "net of things (IoT).[14]

The internet of factors (IoT) is the capacity for devices to communicate with each other thru the net or different networks, retaining song of records remotely and presenting remarks that may assist with choice-making for enterprise, enterprise, and house functions. In fashionable, sensors linked to a lower back-to-base device serve this purpose.

The time period "net of things" refers to products, hardware, or devices with electronics, sensors, firmware, and software program that could store, accumulate, and transmit information to different merchandise or platforms over the net.[14]

B. Artificial Intelligence Roadmap:

The advancement of AI in identifying cybersecurity intrusions within IoT systems is briefly outlined in this section. The techniques have been divided into categories based on the cyberthreats they identify, including Probe, U2R, R2L, and DoSusing attack categories as the foundation for artificial intelligence techniques.[4]

Using artificial intelligence to detect probe attacks Data is collected for probe attacks utilising an external network source, such as portsweep or IPsweep. A peer network's data become available as a consequence of seeking attacks, making it possible for attackers to spy on users, gain access to systems, or collect data. Artificial intelligence methods can be utilised to detect this attack. For example, Zhang et al. indicated an IDS model which employs a deep belief network (DBN) and a genetic algorithm (GA) to obtain a high detection rate in IoT systems. The study also proposed an effective intrusion detection system that can rapidly recognise attacks utilising hybrid artificial intelligence (AI) techniques such as RF, Naive Bayes, C4.5, and REPTree algorithm.[4]

II. Applications of IoT:

The concept of the Internet of Things (IoT) revolves around the connectivity of everyday devices to the internet, enabling independent communication with networks and other devices. This interconnectedness has the potential to enhance various aspects of our lives, businesses, and the environment by leveraging the information provided by these devices. Presently, there are approximately 30 billion active IoT devices, with this number continually increasing each year. This substantial quantity of IoT devices results in a vast amount of collected data, commonly known as Big Data, which necessitates effective control, security, and analysis. Consequently, cybersecurity plays a vital role in safeguarding the IoT ecosystem.[14]

The term "cyber" in cybersecurity pertains to matters concerning information technology, data transmission, and computer systems. Essentially, cybersecurity involves protecting computer systems, mobile and electronic devices, networks, servers, programs, and data from unauthorized access, damage, or attacks. In the cyber world, data encompasses various forms such as numerical data, text, images, audio, and video, all of which can be digitized. These data repositories may contain a wealth of personal information, including a user's background, conversations, locations, and interests. Moreover, they may encompass sensitive personal data like educational or medical records, employment and financial details, online information, and identity.[14]

III.ROLE OF ARTIFICIAL INTELLIGENCE IN IOT (CYBER SECURITY):

A better level of accessibility, integrity, availability, scalability, secrecy, and interoperability in terms of device connectivity has been made possible by the IoT idea. But because of their numerous attack surfaces, newness, and consequent lack of security standards and regulations, IoTs are susceptible to cyberattacks.

Depending on the component of the system being attacked and what the attacker hopes to gain from the attack, there are a wide range of cyberattacks that can be used against IoTs. As a result, a lot of research has been done on IoT cybersecurity. This includes artificial intelligence (AI) methods for defending IoT systems from attackers, typically in the form of seeing peculiar behaviour that would suggest an assault is taking place. However, in the case of IoT, cybercriminals always have the advantage because they only need to uncover one weakness, whereas cybersecurity specialists need to secure several targets. Due to the complex algorithms that detect aberrant behaviour and allow it to go unnoticed, this has also led to a surge in the use of AI by cyberattackers. Due to the expansion of IoT technologies, AI has drawn a lot of attention. With this expansion, AI technologies, including decision trees, linear regression, machine learning, support vector machines, and neural networks, have been applied in IoT cybersecurity applications to be able to recognise dangers and prospective assaults.[14]

IV. Relation between AI and IOT

The purpose of the relationship between AI and IoT:
The Real Value of IoT is in the ability to identify significant patterns in generated data and base decisions or predictions on those patterns. Without employing AI-driven Bigdata processing, it is impossible. Without AI, IoT is a static technology that speeds up device connections and automates data collection. Real smart devices with the capacity for decision-making, self-improvement, and learning can be made using AI and IoT. The use of AI technologies in conjunction with IoT enabled devices can enhance preview solutions and produce amazing goods. An intriguing example of how Google AI and IoT-enabled smart home gadgets might work together is Google Home with voice capabilities. With their voices, people can operate household equipment. IoT applications can be made attractive, economical, and real-time by integrating AI into edge devices, or edge AI. The embedded AI in smartwatches, which can identify a heavy fall and contact emergency services, is a great example.

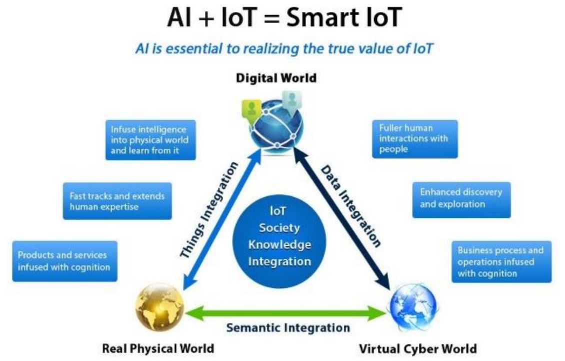
AI + IoT = Smart IoT
AI is essential to realizing the true value of IoT
Digital World
Infuse intelligence into physical world and learn from it
Fuller human interactions with people
Fast tracks and extends human expertise
Enhanced discovery and exploration
Products and services infused with cognition
Business process and operations infused with cognition
Things Integration
Data Integration
IoT Society Knowledge Integration
Semantic Integration
Real Physical World
Virtual Cyber World

Fig. 2: Relation between AI and IoT [23]

1. Cyber Security:

A. IoT Security Threats:

[2] The bulk of IoT hazards are commonplace and low-risk, but a few have a large impact and may cause significant harm.

One significant risk is the potential for hackers to access private data kept on IoT devices. Personal information (such as names, addresses, and passwords), financial information (such as bank account numbers and credit card details), or even sensitive military information (such as troop movements and strategic plans) may fall under this category.

The potential for rogue devices to be set up on company networks or inside of governmental organisations represents another serious hazard. These tools could be used to infiltrate other systems and steal private data.

IoT devices can also be used by hackers to target other systems via the internet of things. This may entail getting access to confidential information, stealing cash or data, or assaulting vital infrastructure systems.

IoT security threats may take a variety of forms, ranging from straightforward password breaches to more complex attacks that take advantage of vulnerability flaws in IoT hardware.[1]

B. AI Helps Cybersecurity Professionals Protect IoT:

Modern AI techniques are used by the cybersecurity sector to maintain its advantage over IoT attacks.

Machine learning (ML) is an application of artificial intelligence (AI) that tells computers to process data and test hypotheses about the data to acquire a "understanding" of it. If the ML algorithms are given the proper working parameters and high-quality data, they can produce meaningful analyses.

One well-liked algorithm for IoT security is naive Bayes. It categorises data based on aberrant activity in the data, which are presumed to result from separate occurrences rather than a single attack. The algorithm, which is named after the Bayesian theorem on which it is based, must first be taught by human overseers before setting its target classifications of activity. After that, it may be left to its own devices on real datasets to detect and flag suspicious and potentially malicious conduct.

With the use of artificial intelligence (AI), decision trees can create complex sets of rules rather automatically. They receive human supervision during training and analyse each piece of data in accordance with an iterative set of rules that ultimately yields a conclusion (typically to a straightforward binary question like "attack or normal").

Some decision tree-based AIs use rule-learning approaches to create their rule sets automatically. An increase in computing power, including novel computer architectures like quantum computing, has allowed for an increase in the artificial "agency" that is being created.

K-nearest neighbour (k-NN) approaches produce classifications based on the Euclidean distance between fresh pieces of data and material that has previously been categorised in the dataset. When kNN algorithms are built, they can start working to find patterns in huge datasets by configuring a geometric proxy.

Artificial neural networks (ANNs) employ a mathematical equation to read vast amounts of input and output goal values through a number of repeated steps across nodes in the network. Although the similarities to real brains are more illustrative than informative, the way electric signals move across synapses in brains served as the inspiration for this strategy.

As fresh information is provided to ANNs, they are able to modify their decision-making models and analysis frameworks. As a result, they are more flexible and dynamic than other AI security solutions when it comes to adjusting to new strategies.[3]

C. Cutting Edge AI for IoT Security:

Today's IoT security is being advanced through AI research. ANNs have been released for anomaly detection, sending data to human engineers for review. Researchers have also suggested AI as a potential way of security control for the IoT, discovering and assessing the consequences of security breaches.

It is obvious that the Internet of Things needs to be cared for while it is still a young technology. AI tools are essential for ensuring the security of the IoT and enabling it to realise its full potential.

D. IoT Security Solutions:

Finally, it's crucial to stay current on the security risks posed by IoT devices and to put the right security measures in place to shield them from assaults. This guarantees that the devices are correctly set up, secure from assaults, and that private data is not jeopardised.

There is no one solution that can shield all IoT devices from all dangers, but there are a few common tactics that can assist to lessen the hazards that these devices present.

A single method should be used to ensure that all IoT devices are configured and secured properly. Setting up user accounts and passwords, configuring firewalls and antivirus programmes, and applying security updates all frequently fall under this category.

Using secure wireless networks to link IoT devices to business networks or governmental systems is an alternative strategy. This prevents the transmission of critical data over unprotected networks and helps defend these systems against attackers.

E. **Different Attacks**:

AI for Detecting U2R Attack:

User to root (U2R) attacks, such as those using perl and xterm, try to gain access to computers as regular users. U2R attacks have the potential to manipulate, spy on, or stop regular system operation. In Bagaa et al., a unique SVM model was suggested based on a security architecture to enable mitigating various vulnerabilities, such as U2R in IoT systems. Additionally, a GA has been suggested for developing criteria to identify U2R threats.[4][15]

AI for Detecting R2L Attack:

Remote to user (R2U) attacks happen when a user transmits packets to a system to which they do not have authorised access, like xclock and guest password. Attacks using R2L take use of system privileges. Chatterjee and Hanawal are two AI techniques for R2L attack detection. In the paper, a federated learning IDS based on a probabilistic hybrid ensemble classifier (PHEC) employing KNN and RF was presented to centralise IoT security. Additionally, a GA was suggested for developing rules to identify R2L assaults.[4][15]

AI for Detecting DoS Attack:

Due to its simplicity of execution, denial of service (DoS) attacks is among the most frequent. Using DDoS attacks and UDP storms, for example, one can disrupt network traffic. DoS attacks have the consequence of overusing system resources, which makes it difficult to handle legitimate networking requests. To detect DoS assaults in IoT Botnets datasets, an AI detection model has been suggested employing several ML/DL techniques, such as CNN, RNN, and SVM.[4][15]

2. Challenges Cybersecurity Faces Today:

Despite breakthroughs in cybersecurity, attacks are getting riskier and riskier.

The primary difficulties with cybersecurity include:

- Geographically remote IT systems—manual incident tracking is made more difficult by distance.
- To successfully track occurrences across geographies, cybersecurity specialists must get over infrastructure gaps.
- Manual threat hunting—can be expensive and time-consuming, leading to more undetected attacks.
- Cybersecurity has a reactive character; businesses can only fix issues after they've already occurred.
- A major difficulty for security professionals is foreseeing dangers before they materialise.
- Hackers frequently alter their IP addresses and conceal them; they do this by using tools like Virtual Private Networks (VPN), proxy servers, Tor browsers, and other tools. Hackers can remain covert and undiscovered with the use of these programmes.[5][15]

3. Benefits of AI in cyber security

A. How AI Improves Cybersecurity

Threat hunting Signatures or indicators of compromise are used in traditional security procedures to recognise threats. This method might be successful against threats that have already been experienced, but it is ineffective against threats that have not yet been identified.

90% of threats can be found using signature-based techniques. AI can improve detection rates up to 95% while replacing conventional methods, but there will be a huge rise in false positives. Combining both conventional techniques and AI would be the ideal course of action. This could lead to a 100% detection rate and reduce false positives.

Employing behavioural analysis with AI can help businesses improve their threat hunting procedures.

By analysing large amounts of endpoint data, you may, for instance, use AI models to create profiles of every application on a network within an organization.[8][19]

B. Vulnerability management

In 2019, 20,362 new vulnerabilities were disclosed, a 17.8% increase from 2018. With so many new risks appearing every day, organisations are having difficulty managing and prioritising them.

Traditional vulnerability management techniques frequently wait for hackers to exploit high-risk vulnerabilities before addressing them.

While traditional vulnerability databases are essential to managing and containing known vulnerabilities, AI and machine learning techniques like User and Event Behavioural Analytics (UEBA) can analyse the normal behaviour of user accounts, endpoints, and servers and identify anomalous behaviour that might signal a zero-day unknown attack. This can aid in protecting organisations even before vulnerabilities are formally identified and patched.[19]

C. Data centers

Numerous crucial data centre operations, including backup power, cooling filters, power consumption, internal temperatures, and bandwidth usage, can be optimised and monitored by AI. Artificial intelligence (AI) has the ability to calculate and continuously monitor, which gives it insights on what factors would increase the efficiency and security of hardware and infrastructure.

AI can also lower the cost of hardware maintenance by informing you when the equipment needs to be fixed. These warnings provide you the opportunity to fix your equipment before it suffers more serious damage. In fact, after adopting AI technology in data centres in 2016, Google reported a 40% drop in cooling expenses at their facility and a 15% drop in electricity use.

D. Network security

Creating security policies and comprehending the network geography of an organisation are two time-consuming parts of traditional network security.

Policies: Security policies help you choose which network connections are safe to use and which you should investigate further for possible malicious activity. These rules can be used to successfully impose a zero-trust model. Because there are so many networks, developing and sustaining policies is the actual issue.

Topography—the vast majority of organisations don't use the same naming standards for their apps and workloads. Security teams must therefore spend a lot of time figuring out which set of workloads are associated with a particular application.

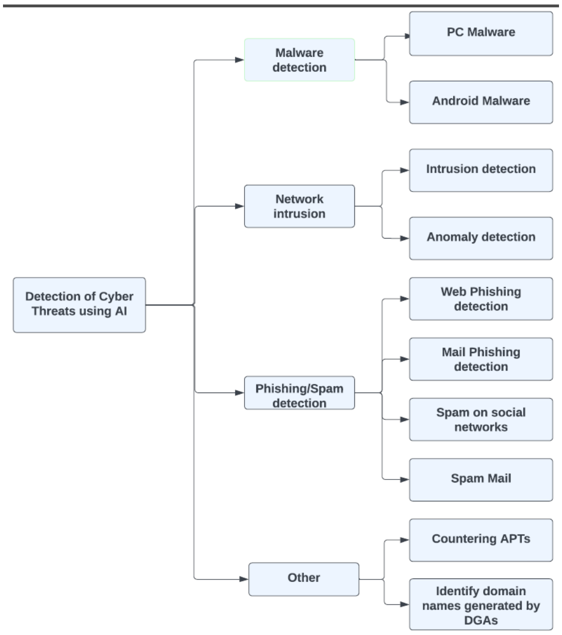

Fig. 3: Benefits of AI in Cyber Security

4. Drawbacks and Limitations of Using AI for Cybersecurity

There are also some limitations that prevent AI from becoming a mainstream security tool:

Resources – In order to create and operate AI systems, businesses must spend a significant amount of time and money on resources like processing power, memory, and data.

Data sets—Learning data sets are used to train AI models. The data sets of malicious codes, malware codes, and abnormalities must be obtained by security teams from a variety of sources. Some businesses just lack the time and funding necessary to compile all of these reliable data sets.

Hackers also employ AI- they refine and test their malware to make it immune to AI-based protection measures. Hackers can design more complex attacks and target both conventional security systems and systems that have been enhanced by AI by learning from the tools that already exist in AI.

Neural fuzzing: Fuzzing is the technique of subjecting software to extensive testing with a large number of random inputs in order to find any weaknesses. AI is used to swiftly test a lot of random inputs through neural fuzzing. Fuzzing does, however, have a positive side. By using the strength of neural networks to gather data, hackers can discover a target system's vulnerabilities. Microsoft created a mechanism to implement this strategy in order to enhance their software, producing more secure code that is more challenging to breach.[6][8]

5. AI with IoT in Health care to treat COVID:

More than 200 countries and territories have been impacted since the first report of Coronavirus Disease 2019 (COVID-19) at Wuhan, China in December 2019. Science and innovation are assuming a crucial role in this perplexing battle. For instance, China focused on computerised reasoning from the beginning of the outbreak when it began its response to infection, relying on facial recognition cameras to follow the infected patients with movement antiquity, robots to deliver food and medications, automatons to clean open spaces, and to watch and transmit sound messages to the general public urging them to stay at home. In order to help COVID-19, artificial intelligence has been widely used to locate additional particles while it is travelling. In addition to certain software engineering analysts focusing on finding the irresistible patients through clinical picture preparation like X-beams and CT filters, many medical professionals are using AI to find new treatments and medications for the problem. In any case, programming created by computer-based intelligence resembles checking armbands and aids in the grouping of individuals while circumventing the isolation rule.Modern smartphones and AI-enhanced thermal cameras are also being used to identify fever and contaminated people. Nations like Taiwan disobeyed the COVID patients based on their mobility history and side effects by combining the public clinical protection information base with contributions from the migration and customs data collection. All in all, AI is used to identify, monitor, and predict flare-ups and aid in infection diagnosis. It is used to manage the claims for medical care. Robots and automatons are used to sanitise public areas as well as transport food and medical supplies. Using super PCs, artificial intelligence is assisting in the development of COVID antibodies and pharmaceuticals. The focus of the current inquiry is on how using artificial intelligence may help the fight against the coronavirus plague. It provides a thorough analysis of the cutting-edge strategies employed to lessen and mask the significant impact of the upheaval. The goal of the current inquiry is to not only assess the effectiveness of the tactics that are shown, but also to advocate for their continued use. This essay explores AI's potential applications and offers a basic vision of how contemporary innovation might combat the COVID-19 epidemic.[7]

V. CONCLUSION

In conclusion, the intersection of Artificial Intelligence (AI) and the Internet of Things (IoT) holds great potential for enhancing cybersecurity measures. The complex and evolving nature of IoT systems makes them vulnerable to various cyber threats. However, with the application of AI techniques such as machine learning and neural networks, cybersecurity professionals can detect and mitigate attacks more effectively. AI-driven anomaly detection, behavioural analysis, and vulnerability management can strengthen the security of IoT devices and networks. By leveraging AI in cybersecurity, organizations can stay ahead of emerging threats, improve threat hunting capabilities, and optimize the protection of data centers and network infrastructure. Embracing the synergistic relationship between AI and IoT is crucial in safeguarding the IoT ecosystem and realizing its full potential.

VI. REFERENCES

[1]. Murat Kuzlu · Corinne Fair · Ozgur Guler-Role of Artifcial Intelligence in the Internet of Things (IoT) cybersecurity https://link.springer.com/article/10.1007/s43926-020-00001-4

[2]. DINESH DAMOR- IoT Security Threats and Solutions IoT Security Threats and Solutions (einfochips.com)

[3]. Ben Pilkington- Using AI to Reduce Iot Vulnerabilityhttps://www.azom.com/article.aspx?ArticleID=21271#:~:text=AI%20Helps%20Cy

[4]. Mujaheed Abdullahi ,ORCID,Yahia Baashar ,ORCID,Hitham Alhussian ,Ayed Alwadain ,Norshakirah Aziz ,Luiz Fernando Capretz ORCID andSaid Jadid Abdulkadir -Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review https://www.mdpi.com/2079-9292/11/2/198

[5]. Eddie Sega -The Impact of AI on Cybersecurity https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity

[6]. Zhibo Zhang; Hussam Al Hamadi; Ernesto Damiani; Chan Yeob Yeun; Fatma Taher -Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research https://ieeexplore.ieee.org/document/9875264

[7]. G Yashodha ,P R Pameela Rani ,A Lavanya and Sathyavathy -Role of Artificial Intelligence in the Internet of Things – A Review https://iopscience.iop.org/article/10.1088/1757-899X/1055/1/012090/pdf

[8]. Jamie Grogan-What's the place of AI in Cybersecurity? https://www.reach-velocity.ai/post/what-s-the-place-of-ai-in-cybersecurity

[9]. The role of Artificial Intelligence in Internet of Things https://www.geeksforgeeks.org/the-role-of-artificial-intelligence-in-internet-of-things/

[10]. Temechu G. Zewdie, Anteneh Girma -IOT Security and the Role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing Environment https://www.nist.gov/system/files/documents/2020/07/13/Temechu-IoT%20Security%20_%20Final.pdf

[11]. Ashish Ghosh∗, Debasrita Chakraborty, Anwesha Law -Artificial Intelligence in Internet of Things https://www.researchgate.net/publication/328223360_Artificial_Intelligence_in_Internet_of_Things

[12]. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity https://link.springer.com/article/10.1007/s43926-020-00001-4

[13]. Tom Nolle -AI and IoT: How do the internet of things and AI work together? https://www.techtarget.com/iotagenda/tip/AI-and-IoT-How-do-the-internet-of-things-and-AI-work-together

[14]. https://www.oracle.com/in/internet-of-things/what-is-iot/

[15]. https://www.tandfonline.com/doi/full/10.1080/08839514.2022.2037254

[16]. https://www.nist.gov/system/files/documents/2020/07/13/Temechu-IoT%20Security%20_%20Final.pdf

[17]. https://www.studytonight.com/post/artificial-intelligence-vs-machine-learning-vs-deep-learning

[18]. https://www.tutorialspoint.com/artificial_intelligence/index.htm

[19]. https://www.javatpoint.com/artificial-intelligence-ai

[20]. https://www.javatpoint.com/iot-internet-of-things

[21]. https://www.tutorialspoint.com/internet_of_things/index.htm\

[22]. https://www.studytonight.com/post/internet-of-things-iot-security-4-critical-challenges

[23]. AIoT = Artificial Intelligence of Things — How #AI and #Automation connect with #IoT: http://bit.ly/2Hr6pTC #BigData #DataScience #MachineLearning #MachineIntelligence #PredictiveAnalytics #EdgeAnalytics #IIoT #Industry40 #DigitalTransformation Graphic: http://cortexlogic.com/aiiot/ https://t.co/nbkw2hlzsB (in-two.com)

Cite this article as :

Mrs. Rashmi Pandey, Ayush Sharma, Devansh Kulshrestha, Devraj Singh Tomar, Dhwaj Sharma, "IntelliGuard: Protecting IoT from AI-driven Cyber Attacks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.389-397, May-June-2023. Available at doi : https://doi.org/10.32628/CSEIT2390388
Journal URL : https://ijsrcseit.com/CSEIT2390388