International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Comparing the Performance of Artificial Intelligence Techniques for Internet of Things Security

[1]Vishwesh Nagamalla
[1]Research Scholar, Department of Computer Science Engineering, Mansarovar Global University, Sehore, Madhya Pradesh

[2]Dr. Akash Saxena
[2]Supervisor, Department of Computer Science Engineering, Mansarovar Global University, Sehore, Madhya Pradesh

ABSTRACT

The use of AI into IoT security has become an important step forward, greatly improving the capacity to identify, stop, and react to cyber-attacks in a digital environment that is very interdependent. Cyberattacks on IoT devices have become more common as their number has grown, highlighting the necessity for strong security protocols. There needs to be strong detection and mitigation strategies developed since the proliferation of Internet of Things (IoT) devices has brought huge security risks. This research looks at how well four different AI methods—Support Vector Machine (SVM), Decision Tree, Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM)—handle security risks associated with the Internet of Things (IoT). These models were trained and evaluated using publicly accessible datasets, such as CICIDS2017, NSL-KDD, and UNSW-NB15. Important measures including F1-score, recall, accuracy, and precision were used to evaluate the efficacy of each AI method.

Keywords: Security, Artificial Intelligence, Accuracy, Precision, Support Vector Machine

I. INTRODUCTION

A revolutionary technology, the Internet of Things (IoT) is changing many parts of people's lives and businesses' day-to-day operations. The Internet of Things (IoT) intends to automate and streamline once inconceivable processes by linking disparate devices and systems, such as wearable gadgets, industrial sensors, and home appliances. Smart homes, healthcare, transportation, and manufacturing are all benefiting from this connection as it allows for remote monitoring and control as well as real-time data collecting. To protect personal information and society at large, however, there are serious security concerns brought about by the fast expansion of IoT devices and their incorporation into vital infrastructure. Internet of Things (IoT) is essentially just a term for a system of interconnected computing devices that may collect and share data via an existing network of internet-connected hardware, software, and sensors. From simple home appliances like smart thermostats and security cameras to advanced infrastructure like smart grids and industrial robots, these technologies cover the gamut. Advanced functionality and insights that were previously unreachable are made possible by the linked nature of the IoT, which provides a broad ecosystem in which data flows easily between devices, apps, and people.

Internet of Things (IoT) has the potential to improve operational efficiency and decision-making by providing data-driven insights. In the energy sector, smart grids analyze consumption patterns in real time to improve distribution, while in the medical field, wearable health gadgets allow for continuous monitoring of vital signs, which may lead to early diagnosis of medical disorders. Internet of Things (IoT) sensors can foretell when machinery will go down, cutting down on repairs and downtime in industrial settings. These developments highlight the revolutionary potential of the Internet of Things, which may lead to substantial enhancements in operational efficiency and quality of life. The Internet of Things (IoT) has many benefits, but its size and complexity also make it a security risk. Security flaws are more likely to be exploited due to the large attack surface created by the sheer quantity of linked devices. Because of limitations in resources like computing power, energy consumption, and price, many IoT devices come with bare-bones security measures. Consequently, they are prone to assaults since

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

they do not have strong authentication methods, encryption, or frequent software upgrades.

Unauthorized access to networks and devices connected to the internet is a big security problem. Because consumers seldom update the default or weak passwords on their IoT devices, these devices are susceptible to brute-force assaults. Once an intruder gets their hands on a device, they may use it to steal information or take over other devices on the network. A hacked smart thermostat or security camera, for example, might be used to monitor a user's house or interfere with HVAC systems. The risk of data breaches and privacy abuses is another major obstacle. Internet of Things (IoT) devices produce massive volumes of data, which may include sensitive information, habits, and even weather conditions. Malicious actors may intercept, access, or steal this data if it is not adequately protected. Serious repercussions, such as financial loss, reputational harm, and identity theft, may result from data breaches. Take wearable gadgets as an example. If there's a data breach, critical medical information might be exposed, which could lead to privacy breaches and data exploitation.

Problems in protecting data integrity and communication routes are another consequence of the intricate nature of IoT networks. Depending on the protocol or network that an IoT device is communicating across, there may be different security considerations. It is possible to intercept or alter data in transit by taking advantage of insecure communication links. Data integrity is also critical for keeping information used for decision-making accurate and reliable. False information or attempts to manipulate sensor data by attackers might lead to erroneous conclusions and harmful outcomes. Security for the Internet of Things is already a formidable obstacle, and the ever-changing nature of cyber threats only makes things worse. Maintaining up-to-date security measures and constantly monitoring for any threats is crucial, since new vulnerabilities and attack strategies are always appearing. Unfortunately, there are long-term security vulnerabilities associated with many IoT devices since they were not built with future upgrades in mind. Addressing these difficulties is made more complicated by the fact that various manufacturers and types of IoT devices do not adhere to common security methods and procedures.

Managing vulnerabilities and applying software patches is another essential part of Internet of Things security. The embedded software that powers many IoT devices could have security flaws. To fix these problems and safeguard against newly found threats, updates and patches need to be applied regularly. The vast number of devices, the variety of update protocols, and the possibility of service interruptions all make update deployment a difficult task. The security and timely updates of all devices depend on the users, service providers, and device makers working together effectively. Security breaches in IoT systems have the potential to have far-reaching implications, impacting not just users but also vital infrastructure and public safety. For example, traffic congestion, accidents, and delays might result from a cyberattack on smart transportation networks. Similarly, whole towns may be affected if smart grid systems were to be breached, leading to power outages or affecting energy distribution. The need for strong security measures to safeguard vital services and prevent such attacks is brought to light by the incorporation of IoT into critical infrastructure.

II. REVIEW OF LITERATURE

Ahanger, Tariq et al. (2022) There has been a lot of focus from the innovation community on the data privacy issue related to the IoT paradigm. Various studies have addressed various concerns related to the Internet of Things (IoT), such as intrusion detection systems, vulnerability modeling, and the most recent methods proposed for this purpose. On the other hand, in our study, we only focus on new Internet of Things vulnerabilities and associated artificial techniques. This study establishes the groundwork for a comprehensive classification of current studies that investigate various ML and DL approaches for the Internet of Things (IoT) paradigm. Weak connections, potential solutions, and existing corporate authentication systems that may identify and monitor these vulnerabilities are all part of the new taxonomy that is based on IoT vulnerabilities, associated attackers, and impacts. In order to help readers achieve their repair objectives, this article aims to provide a multi-dimensional analytical perspective on Internet of Things (IoT) vulnerabilities, including technical details and consequences. Motivated by the dearth of scientific (and malevolent) proof pertaining to the Internet of Things paradigm, the present research focuses on manipulating the IoT via passive measures. This study not only provides organizational knowledge resources that will help with the mitigation goal overall, but it also shows how severe the Internet of Things situation is. Current study reveals not just open challenges and research concerns, but also instructive findings, inferences, and outcomes. These will guide future research activities aimed at resolving scientific concerns related to the security of the Internet of Things.

Abed, Ali & Anupam, Angesh. (2022) The Internet of Things (IoT) is a system that is composed of many software and hardware components that relies on internet services and various cutting-edge sensing and communication technologies. The advent of 5G technology will cause the Internet of Things (IoT) to expand even farther over the globe, but there are security issues with IoT that need careful analysis as well. The article will provide a comprehensive overview of the security difficulties faced by an IoT network, including current assaults on IoT technology, communication protocols often used in IoT systems, and the role of AI in IoT security. All the key aspects of Internet of Things security, including possible AI-based solutions, are discussed and assessed in one place for the first time. This study provides valuable insights for future research on improving IoT communication protocols and developing AI tools to address privacy and security concerns in the IoT.

Kane, Luke et al., (2020) The security and performance of these low-power devices are of paramount significance, especially considering that forecasts indicate there will be 18 billion IoT devices online by 2022. We must strike a balance between security and performance while managing. Finding that sweet spot will be difficult forever. There are two primary benefits to this region from this study. An approach to gauging the security of Internet of Things devices is the first contribution. The categories that are measured include power consumption, time cost, energy cost, RAM utilization, and flash usage. Insightful comparisons of the performance of low-powered microcontroller devices such as the ATmega328, STM32F103C8T6, and ESP8266 are shown in the second contribution. We conducted experiments on these devices with different cryptographic procedures. Three different crypto algorithms—Advanced Encryption Standard (AES), ChaCha, and Acorn—had their operations measured. This study's suggested methodologies are applicable to actual, rather than hypothetical, Internet of Things (IoT) performance assessment and may be used by anyone interested in doing so. The findings reveal that, when looking at total power usage, the ATmega328 is the most efficient. Typically, the device with the best performance was the ESP8266. In terms of energy cost and time cost, ChaCha was superior than AES. In these measures, both algorithms fared better than Acorn. When comparing devices, the STM32F103C8T6 showed the best overall energy cost and time performance. Network designers, developers, and others may use the study's experimental findings to make informed judgments about balancing performance and security in IoT installations.

Hui, Wu et al., (2020) A wide range of cutting-edge integrated solutions for various uses have emerged from the Internet of Things (IoT), which has evolved along three main trajectories: authentication, communication, and computation. Nevertheless, every layer of the three-tiered IoT architecture is vulnerable to different security risks because of the openness, expansivity, and resource limitations of the IoT. We discover that AI techniques like Deep Learning (DL) and Machine Learning (ML) may provide new strong capabilities to satisfy the security needs of the Internet of Things (IoT) after conducting a comprehensive analysis of the particularity and complexity of IoT security protection. We provide a high-level overview of the basic procedure for AI solutions to IoT security issues and assess the technological feasibility of AI in doing so. We summarize representative AI solutions and compare the different algorithms and technologies used by various solutions for four serious IoT security threats: device authentication, defense against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, intrusion detection, and malware detection. It is important to remember that although AI does provide a lot of new features to help keep the Internet of Things secure, it also brings a lot of new problems and risks to the table in terms of data, algorithms, and design. Possible future research areas may be based on how to tackle these difficulties.

Surya, Lakshmisri. (2019) To combat threats including eavesdropping, jamming, denial of service (DOS), and spoofing, as well as other forms of cybercrime, the internet of things (IoT) connects different network devices to provide smart and sophisticated services. This study delves into the methodology used by IoT systems in conjunction with AI to bolster the safety of connected devices. The study goes on to discuss machine learning-based solutions for Internet of Things security, including supervised learning, unsupervised learning, and reinforcement learning. Machine learning (AI) based authentication methods, safe offloading, access control, and virus detection for the Internet of Things are among the main topics of this article. Furthermore, the article discusses the difficulties that must be studied and overcome in order to put these machine learning security strategies into practice in IoT systems. The Internet of Things (IoT) is being heralded as the catalyst for the next technological revolution. This new technology is expected to bring about cellular network networks, simple accessibility across highly secure and dynamic services, and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

context awareness. As a result, AI has the potential to have a big impact on network infrastructure technologies. Nevertheless, certain issues will emerge as a result of using AI principles, instruments, and technologies in cellular connections used by the IoT. This article discusses the important problems with artificial intelligence (AI) in wireless information systems that allow end-to-end Internet of Things (IoT) connection, as well as potential solutions and areas for future study.

Xiao, Liang et al., (2018) Protecting user privacy and addressing threats like spoofing, denial of service (DoS), jamming, and eavesdropping are important concerns for the Internet of Things (IoT), which connects various objects to networks to provide smart and enhanced services. We examine the Internet of Things (IoT) threat model and survey the IoT security solutions built on ML approaches, such as RL, unsupervised learning, and supervised learning. Protecting data privacy using machine learning-based strategies for authentication, access control, secure offloading, and malware detection in the Internet of Things (IoT) is the purpose of this article. Additionally, we go over the obstacles that must be overcome in order to apply these ML-based security measures to real-world Internet of Things systems.

III. RESEARCH METHODOLOGY

Dataset Selection

The research made use of CICIDS2017, NSL-KDD, and UNSW-NB15, three open-source IoT security datasets.

Model Implementation

The following artificial intelligence models were used: Support Vector Machine (SVM), Decision Tree, Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM).

Evaluation Metrics

We used F1-score, recall, accuracy, and precision to evaluate the AI methods.

IV. RESULTS AND ANALYSIS

Table 1: Performance Comparison

AI Technique	Accuracy	Precision	Recall	F1-Score
Support Vector Machine (SVM)	92.3%	90.1%	88.7%	89.4%
Decision Tree	89.7%	87.5%	85.3%	86.4%
Convolutional Neural Network (CNN)	94.8%	92.7%	91.5%	92.1%
Long Short-Term Memory (LSTM)	93.5%	91.2%	89.8%	90.5%

The Convolutional Neural Network (CNN) achieves the best accuracy of 94.8% compared to the other methods, showing that it is more capable of accurately classifying cases. It has a high percentage of genuine positive predictions among all positive categories and leads in precision at 92.7%. With a recall of 91.5%, CNN proves to be quite good at picking out genuine positives out of all the false positives. The overall performance of CNN, which successfully balances recall and precision, is further highlighted by its F1-score of 92.1%. Next on the list is Long Short-Term Memory (LSTM), which comes in at 93.5% accuracy and a solid 90.5% F1-score. Although it is marginally less effective than CNN, LSTM is still capable of detecting threats with a recall of 89.8 percent and an accuracy of 91.2 percent. According to the results, LSTM excels at processing sequential data, which makes it a promising candidate for time-series analysis in the context of Internet of Things security.

With a recall of 88.7 percent, a precision of 90.1 percent, and an accuracy of 92.3 percent, the Support Vector Machine (SVM) shows good performance. Its balanced performance is shown by the F1-score of 89.4%, which is slightly lower than CNN and LSTM. Despite being less successful than CNN and LSTM, SVM's performance in

high-dimensional domains demonstrates its capabilities. Among the four methods, the Decision Tree performs the worst, with a recall of 85.3%, precision of 87.5%, and accuracy of 89.7%. Although it has a cheap computing cost and is helpful for smaller tasks, its F1-score of 86.4% shows that it is not as good as the more complicated models at reliably detecting security risks to the Internet of Things.

V. CONCLUSION

Machine learning techniques, like as decision trees and neural networks, show great potential in identifying abnormalities and possible threats since they can learn from extensive datasets and adjust to changing attack methods. On the other hand, rule-based systems and expert systems offer reliability and clarity but may not have the flexibility of more dynamic AI techniques. Utilizing AI strategies that combine predictive accuracy and flexibility, together with continuous breakthroughs in AI research, is essential for improving IoT security. In summary, a hybrid approach that leverages the advantages of several AI approaches is the most efficient strategy for tackling the intricate and constantly evolving realm of IoT security risks.

REFERENCES: -

[1] T. Ahanger, A. Aljumah, and M. Atiquzzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," *Comput. Networks*, vol. 206, no. 2, pp. 10-71, 2022, doi: 10.1016/j.comnet.2022.108771.

[2] Abed, A. Ali, and A. Angesh, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," *Security and Privacy*, vol. 6, no. 7, pp.10-25, 2022, Art. no. e285, doi: 10.1002/spy2.285.

[3] L. Kane, J. Chen, R. Thomas, V. Liu, and M. McKague, "Security and Performance in IoT: A Balancing Act," *IEEE Access*, vol. 8, no. 9,pp. 1-1, 2020, doi: 10.1109/ACCESS.2020.3007536.

[4] W. Hui, H. Han, X. Wang, and S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, no. 5, pp. 1-1, 2020, doi: 10.1109/ACCESS.2020.3018170.

[5] L. Surya, "IoT Security Techniques Based On Machine Learning: How IoT Devices use AI to Enhance Security," *SSRN Electronic Journal*, vol. 67, no. 2, pp. 65, 2019, doi: 10.14445/22312803/IJCTT-V67I2P110.

[6] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, no. 5, pp. 779–796, 2019, doi: 10.1016/j.future.2019.05.041.

[7] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1285–1297, 2019, doi: 10.1109/TEM.2019.2922936.

[8] R.-H. Hwang, M.-C. Peng, V.-L. Nguyen, and Y.-L. Chang, "An LSTM-based deep learning approach for classifying malicious traffic at the packet level," *Appl. Sci.*, vol. 9, no. 16, pp. 34-44, 2019.

[9] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *Proc. IEEE Pacific Rim Int. Symp. Dependable Comput., PRDC*, vol. 81, no. 7,, pp. 256–265, 2019.

[10] Nagisetty and G. P. Gupta, "Framework for detection of malicious activities in IoT networks using Keras deep learning library," in *Proc. 3rd Int. Conf. Computing Methodologies and Communication, ICCMC*, vol. 9, no. 1, pp. 633–637, 2019.

[11] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, 2018, doi: 10.1109/MSP.2018.2825478.

[12] Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in fog-to-things communications," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 124–130, 2018.

[13] T. Aldwairi, D. Perera, and M. A. Novotny, "An evaluation of the performance of restricted Boltzmann machines as a model for anomaly network intrusion detection," *Comput. Netw.*, vol. 144, pp. 111–119, 2018.

[14] N. Sainis, D. Srivastava, and R. Singh, "Feature classification and outlier detection to increased accuracy in intrusion detection system," *Int. J. Appl. Eng. Res.*, vol. 13, no. 10, pp. 7249–7255, 2018.

[15] Y. Zhou, M. Han, L. Liu, J. S. He, and Y. Wang, "Deep learning approach for cyberattack detection," in *IEEE INFOCOM 2018-IEEE Conf. on Computer Commun. Workshops (INFOCOM WKSHPS)*, vol. 9, no. 1, pp. 262–267, 2018.