International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Comprehensive Survey of Deep Learning-Based Intrusion Detection and Prevention Systems for Secure Communication in the Internet of Things

V. G. SaranyaVaishalini*[1], A. Ramathilagam[2], R. Palanikumar[3], P. Raghavan[4], P. Gopikannan[5], K. Manikandan[6]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract: The Internet of Things (IoT) is a gadget that is connected to many devices that are permitted to detect and collect data from the provided environment and communicate the data over wireless media without any human involvement. IoT is widely used in various applications, namely healthcare, education, agriculture, military applications, etc. Due to its open nature and design, it is vulnerable to various kinds of network attacks. In an IoT environment, security should be stronger in order to prevent malicious activities. The Intrusion Detection System (IDS) was created to identify and prevent various types of harmful assaults on the network. Every organisation needs to manage these kinds of attacks and malicious activities. Many organisations fail to detect and prevent many unknown malicious attacks. So, safeguard measures have to be taken by the organisation in order to provide better security, reliability, and privacy in the IoT environment. In this paper, a survey on security issues related to the methods of deep learning and machine learning was used to analyse vulnerabilities in the IDS network.

Keywords: *Internet Of Things, Intrusion Detection System, Malicious, Reliability, Security*

1. Introduction

The IoT is widely utilised in many fields, which include smart environments, automation, industrial processes, and healthcare [1]. IoT has many benefits and services, but it also has serious security issues. The heterogeneous nature of IoT is not compatible with traditional security mechanisms. But it supports other aspects such as confidentiality, access control, and authentication of data. Even though these security aspects were developed in combination with the end user, IoT still suffers from security problems [2]. Developing a separate module for network security in the IoT is considered a challenging task. The evolution of the Internet has major dominance in developing environments, but it also paves the way for a huge number of security attacks, which need to be addressed to provide a trustworthy environment [3]. IoT advancement is widespread over streets, cities, and buildings that have been connected to sensors to sense the smartness of the environment. IoT is utilised to enhance livelihoods and social networks by safeguarding them from security attacks. IDS [4] is a software or hardware component that detects a security attack by continuously monitoring the system activity and network traffic for any abnormal activity or policy breaches in the system. Once the attack is identified, it reports to the administrator through an alert. The network or host that is connected to the internet is automatically connected to all other computers on the planet, which makes the system more vulnerable and prone to high security risks. IDS continuously monitors the system, folder, or file for security attacks. The literature survey clearly explains the IDS and IPS [5], which are utilised for detecting and preventing security attacks. IDS is a passive monitoring system that alerts the administrator instead of taking action on its own. But IPS is the active monitoring system that takes the necessary action and stops the further functioning of the system. In IPS, the data pattern is taken into consideration and compared with the previously stored data to effectively identify and prevent the intrusion [6]. IDS is considered a source of protection that does not provide safe access control. On the other hand, IPS is able to provide preventative measures in caution with the violation in the network-secured environment when it is connected with the IDS and firewall [7]. IDS prevents intrusion, assaults, and data losses, which are emerging every day, but it is even more difficult for technologies to identify the attacks. Machine learning (ML) [8] methods are used to analyse the vast volume of data, producing rules for identifying events, prediction, and classification. Various applications, such as speech recognition, medical diagnosis, traffic prediction,

[1] *Assistant Professor, Department of Computer Science and Engineering, P. S. R. Engineering College, Sivakasi, Tamil Nadu, India*
Email: vaishalinipsr@gmail.com
[2] *Professor, Department of Computer Science and Engineering, P. S. R. Engineering College, Sivakasi, Tamil Nadu, India*
Email: thilla2012@gmail.com
[3] *Associate Professor, Department of Computer Science and Engineering, P. S. R. Engineering College, Sivakasi, Tamil Nadu, India*
Email: palanikumar@psr.edu.in
[4] *Assistant Professor, Department of Computer Science and Engineering, P. S. R. Engineering College, Sivakasi, Tamil Nadu, India*
Email: raghavan.ramesh1988@gmail.com
[5] *Assistant Professor, Department of Computer Science and Engineering, P. S. R. Engineering College, Sivakasi, Tamil Nadu, India*
Email: gopi.kannan11@gmail.com
[6] *Assistant Professor, Department of Computer Science and Engineering, P. S. R. Engineering College, Sivakasi, Tamil Nadu, India*
Email: manikandan.k@psr.edu.in
** Corresponding Author Email: vaishalinipsr@gmail.com*

and intrusion detection, use ML algorithms. Combining IoT with ML generates an effective result. IDS utilises various ML approaches. Natural language processing, neural networks [9], and ML are techniques of artificial intelligence (AI) [10], which effectively identify and detect intrusions. In this paper, a comprehensive survey of various IDS and IPS techniques, both deep learning and machine learning, is used to highlight their pros and cons and pave the way for future research in the field of IDS in the IoT. Table 1 provides the acronyms and abbreviations used in this paper.

Table 1. Acronyms and Abbreviations

Acronyms	***Abbreviation***
IoT	Internet of Things
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IDPS	Intrusion Detection and Prevention System
ML	Machine learning
NLP	Natural Language Processing
NN	Neural Networks
DL	Deep learning
n-SOINN	Self-Management Incremental Neural Network
WTA	Winner Takes All
SVM	Support Vector Machine
AON	Ad hoc Network Architecture
OVS	Open V switch
SDN	Software Design Networking
DC	Degree Centrality
BC	Betweenness Centrality
CPS	Cyber Physical Systems
IIoT	Industrial Internet of Things
RFM	Random Forest Model
GA	Genetic Algorithm
DT	Decision Tree
ET	Extra-Trees
XGB	Extreme Gradient Boosting
PDAE	Parallel Deep Auto-Encoder
NIDS	Network Intrusion Detection System
MemAE	MemoryAugmented Auto-Encoder
XGB	Extreme Gradient Boosting
ETC	Extra Tree Classifier

2. Literature Survey

IoT cyberattacks are constantly evolving and becoming stealthier; thus, the IDS needs to be regularly updated to protect against newly developed security hazards. The heterogeneity of IoT networks enables the delivery of temporal, multifaceted, and high-dimensional data. Analytics using big data may be used with these types of data to find previously undiscovered patterns, expose hidden correlations, and provide fresh insights. Big data analysis is increasingly utilising artificial intelligence [27]. Deep learning methods are particularly good at handling heterogeneous data. Many scholars who use ML or DL methods reveal IDS on a regular basis. Issues associated with impulsive data cleaning and processing include overfitting, underfitting, and additional issues. The Internet of Things and intelligence detection systems solutions based on deep learning strive to create models with high levels of efficacy and efficiency. But every model has certain architectural decisions that could reduce the possibility that it will be successful in achieving these goals. Some IoT deep learning [28–29] IDSs apply their model to an unbalanced dataset or take account of the overfitting problem, all of which have an adverse impact on their accuracy, memory utilisation, and computation time. Furthermore, some intrusion detection systems do not make an effort to enhance their initial learning model, while others are assessed using out-of-date or inappropriate datasets that do not fairly depict the traffic on IoT networks in the real world. For safety reasons, deep learning is applied to intrusion detection systems and malware detection [30, 31]. The present survey's primary subjects are the ML and DL methods for IDPS.

The authors [11] have developed a sophisticated intrusion prevention system with the intention of accurately mitigating both unknown and known attacks on Internet of Things networks. A slightly altered version of the self-management incremental neural network (n-SOINN) serves as the foundation for the suggested approach. Multiple SVMs are combined with online clustering for classification. Since Support Vector Machine (SVM) helps to handle binary issues, which serve as a classification algorithm to break down a multiclass issue into a number of distinct classification issues, As a result, "n-SOINN & WTA-SVM" is a combination at the foundation of the detection algorithm of the proposed design.

The authors [12] have proposed a novel intrusion prevention approach for the internet of things. A thin-walled networking connection is developed to serve as a WiFi connecting point for residential IoT devices and as a running platform for detection models and security policies. The authors first use Raspberry Pi and the Ad Hoc Network Architecture (AON) to construct cache management and security policies. Additionally, Open V Switch (OVS) for virtual switch capability is running on this gateway. The classification model is trained using the decision tree supervised learning approach, which then extracts features of network traffic to differentiate between authorised and unauthorised traffic designs. The simulation result of the proposed system shows that it can efficiently provide security for home IoT interactions and that its intrusion detection on edge intelligent gateways is very accurate.

Software Design Networking (SDN) has been developed by Gonçalves et al. [13]. As a result, the SDN will be able to stop assaults as close to their origins as feasible, lowering the number of unauthorised activities and disconnecting the affected device from the rest of the network. This will enable the IPS to detect strange behaviours from IoT devices. Snort IDS's primary job is to detect malicious traffic. Validation experiments show that the suggested approach can stop assaults that Snort can detect.

The authors [14] developed a novel intrusion prevention system technique for providing enhanced security in the system. In reality, the intrusion prevention system that has been offered is an analysis of risks that aids in determining the appropriate mitigation strategy for each threat that has to do with authentication, access control, or secrecy. Identification, prioritisation, selection of efficient mitigation strategies, and development of viable cures are all steps in the procedure of developing an intelligent home risk assessment model. Experiences with the suggested method demonstrate its effectiveness in protecting against various dangerous cyber-attacks.

The authors [15] developed an intrusion prevention system for safeguarding the network from unknown and known attacks due to the centralised approach techniques. When compared to traditional technologies, blockchain technology provides better security and authentication where traditional techniques lack dependency on external security, is highly trustworthy, and more.

The authors [16] presented a zero-false-positive IPS for industrial Internet of Things (IoT) and CPS (Cyber Physical Systems) using a power grid security case study. The authors developed an innovative approach to dealing with interruption problems by altering any basic classification into one that generates zero false positives. The output of the algorithm could then be simply converted into a tree-based classifier. The outcomes confirm the strategy's effectiveness. Table 2 provides IPS techniques.

Table 2. IPS techniques

Method	*Detection technique*	*Advantages*	*Limitations*
Automated Progressive Training Intruder Protection System. [11]	The Winner is made up of many SVMs and a Self-Organizing Progressive Neuronal Network.	Provides better accuracy.	The dataset uses more redundant data and unable to predict unknown attacks in the network.
Edge Computing-Based Approach for Intrusion Prevention [12]	Ad hoc Network Architecture (AON) was implemented in the Edge Smart Gateway.	Provides High Accuracy 97.1%	Unable to predict new type of network attacks.
Snort IPS design with SDN [13]	Snort IPS	Quickly scan and detects DoS attack by the use of blocking rules.	Since the blocking rules are signature-based IDS, it cannot find new or zero-day attack.
IPS based on cyber security [14]	Cybersecurity	Efficient and effective in detecting various cyberattacks in the network.	Proficiency was not evaluated
IPS using blockchain technique [15]	Blockchain Techniques	Blockchain technology performs better when compared to SHA-1 algorithm and MD5.	The proposed system has to be compared with SHA-2 for more security.
Machine learning based IPS [16]	Z-classifier	It achieves zero false positives.	The dataset is outdated.

Kasongo [17] developed and evaluated a robust industrial IoT (IIoT) IDS solution utilising the UNSWNB15 dataset. Two stages were used in the development of the IDS. In the initial stage, the Random Forest Model (RFM) and Genetic Algorithm (GA) were employed to choose the most salient characteristics. The testing results showed that, utilising a feature vector with 16 features, the proposed system provides better accuracy and performance when compared to other existing systems.

The authors [18] developed novel decentralised IDS that use fog technology for computing to track or recognise distributed denial of service (DDoS) assaults against mining pools. Regular activities are carried out by hackers participating in a mining pool, and those actions are then uploaded to the blockchain network. The applicability of the proposed methodology is evaluated using a real Internet-based dataset known as BoT-IoT that incorporates the most recent hazards discovered in blockchain-enabled IoT networks. The results of this study show that Random Forest surpasses XGBoost for bipolar identification of attacks, whereas XGBoost surpasses Random Forest for multi-attack detection.

A revolutionary parallel deep auto-encoder (PDAE)-based network intrusion detection system was suggested by Basani and Faghih [19]. The PDAE learning model makes use of local and global knowledge about certain feature vector values. They can significantly decrease the number of parameters, memory footprint, and processing power requirements while enhancing model accuracy because of this kind of feature isolation. The results reveal that the suggested model beats the most advanced algorithms in terms of performance and accuracy.

An automatic machine learning-based intrusion detection system (ML-IDS) was proposed by the authors [20] to detect vulnerabilities in Internet of Things networks. To avoid information from leaking onto the experimental data, feature scaling was performed in the first stage of this study technique on the UNSW-NB15 dataset using the minimum-maximum normalisation idea. The ability of six suggested machine learning models to predict outcomes was evaluated using UNSW-NB15 as a benchmark dataset. Considering an accuracy rating of 99.9% as well as an MCC of 99.97%, the results were determined to be competitive when compared with previous published papers.

A two-stage aggregation method for intrusion detection and identification in fog-based computing and Internet of Things environments was presented by Souza et al. [21]. There are two steps in the proposed IDS: identification and detection. These procedures are used to categorise events as either attacks or non-attacks of a particular type. The data is analysed using the binary Extra Tree Classifier (ETC), which determines whether or not the traffic flow captured by the device is invasive. Non-intrusive traffic is immediately released. The proposed approach was successful in achieving comparable or better performance in all databases, demonstrating its power and effectiveness. Table 3 provides IDS techniques.

Table 3. IDS Techniques

Method	***Detection technique***	***Advantages***	***Limitations***
Robust Industrial IoT (IIoT) IDS solution [17]	Tree-based classifiers include RF, DT, ET, and XGB.	Provides better accuracy and security.	Unable to perform some minority classes in the network.
Intrusion Detection System (IDS) with fog computing [18]	Extreme Gradient Boosting (XGBoost) and Random Forest (RF)	Effectively detects various types of cyberattacks.	Unable to detect unknown attacks.
IDS based on deep learning technique [19]	Parallel Deep Auto-Encoder (PDAE)-based NIDS	High Accuracy and more efficient than other techniques.	Time complexity has to be optimized
IDS based on machine learning technique [20]	CatBoost, XGBoost, SVM algorithms	Better performance with high accuracy.	Computational cost and the consumption of energy has to be concentrated
IDS employ machine learning and supervised learning techniques. [21]	Tree-based classifiers include RF, DT, ET, and XGB.	Achieves high precision and recall rates with better accuracy.	IDS prediction time is high.

Table 4. Comparative assessment of various IDS and IPS techniques

Methods	*Detection rate*	*False positive rate*	*Accuracy*	*Security*	*Efficiency*
Automated Progressive Learning Intrusion Prevention System. [11]	✗	✗	✓	✓	✓
Edge Computing-Based Approach for Intrusion Prevention [12]	✗	✓	✓	✓	✗
Snort IPS design with SDN [13]	✓	✗	✓	✓	✓
IPS based on cyber security [14]	✓	✗	✓	✓	✗
IPS using blockchain technique [15]	✓	✓	✓	✗	✓
Machine learning based IPS [16]	✓	✓	✓	✓	✓
Robust Industrial IoT (IIoT) IDS solution [17]	✓	✓	✓	✓	✗
Intrusion Detection System (IDS) using fog computing [18]	✓	✗	✓	✓	✓
IDS using deep learning approach [19]	✓	✓	✓	✓	✓
IDS based on machine learning technique [20]	✓	✓	✓	✓	✓
IDS employs artificial learning and supervised learning techniques. [21]	✓	✓	✓	✓	✓

3. Comparative Assessment of Various IPS and IDS Techniques

In this section, the comparative assessment of various IPS and IDS techniques based on IoT approaches to deep learning and machine learning is compared based on the performance matrices, namely intrusion detection rate, false positive rate, accuracy, security, and efficiency. Table 4 gives a comparative assessment of various IPS and IDS techniques. The table proves that the IDS and IPS techniques, which are based on deep learning and machine learning, offer improved security, a high accuracy rate for intrusion detection, efficiency, and a false positive rate. The IDS and IPS techniques, which are based on block chain and soft computing approaches, provide better security and efficiency but fail to provide a better intrusion detection rate with good accuracy and a false positive rate.

4. Conclusion and Future Work

In this study, we investigate several models of ML and DL together with ML and DL-based intrusion detection systems and intrusion prevention systems for the Internet of Things. The study examines a number of detection and avoidance methods for intrusions using machine learning and deep learning techniques. The survey briefly examines the pros and cons of the approaches to offer an opportunity for researchers working in this area. According to various classifications based on architecture, locations, and functions, we address the fundamental elements of IDS. The various IDS technologies are also categorized based on the most recent research studies. As there are currently few surveys with a framework and preventative model, our survey helps IDS and IPS developers understand the design process for IDS and IPS methodologies and technologies. The study also examines the most recent IDS models. Each ML and DL model is compared and described in detail using tables. Finally, we have pointed out a few study-related issues and offered some suggestions for further research.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] S. M. Kasongo and Y. Sun, “A deep learning method with wrapper-based feature extraction for wireless intrusion detection system,” Computers & Security, vol. 92, article 101752, 2020.

[2] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, “TSDL: a two-stage deep learning model for efficient network intrusion detection,” IEEE Access, vol. 7, pp.

30373–30385, 2019.

[3] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” IEEE transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.

[4] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, “A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks,” Electronics, vol. 8, no. 11, p. 1210, 2019.

[5] A. Derhab, M. Guerroumi, A. Gumaei et al., “Blockchain and random subspace learning-based ids for sdn-enabled industrial iot security,” Sensors, vol. 19, no. 14, p. 3119, 2019

[6] Y. Otoum, D. Liu, and A. Nayak, “DL-IDS: a deep learning– based intrusion detection framework for securing IoT,” Transactions on Emerging Telecommunications Technologies, no. - article e3803, 2019.

[7] M. Kumar, Deep learning approach for intrusion detection system (ids) in the internet of things (iot) network using gated recurrent neural networks (gru), Wright State University, 2017.

[8] M. Roopak, G. Y. Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” in 2019 IEEE 9th annual computing and communication workshop and conference (CCWC), pp. 452–457, Las Vegas, NV, USA, 2019.

[9] M. Roopak, G. Y. Tian, and J. Chambers, “An intrusion detection system against ddos attacks in iot networks,” in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 562–567, Las Vegas, NV, USA, 2020.

[10] B. Roy and H. Cheung, “A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network,” in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1–6, Sydney, NSW, Australia, 2018.

[11] Constantinides, Christos, Shiaeles Stavros, GhitaBogdan, and Kolokotronis Nicholas. (2019) “A novel online incremental learning intrusion prevention system.” 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1–6.

[12] Jiang, Chao, JianKuang, and Shirui Wang. (2019) “Home iot intrusion prevention strategy based on edge computing.” 2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE), 94–98.

[13] Gonçalves, Daniel GV, et al. (2019) “IPS architecture for IoT networks overlapped in SDN.” 2019 Workshop on Communication Networks and Power Systems (WCNPS), 1–6.

[14] James, Fathima. (2019) “IoTcybersecurity based smart home intrusion prevention system.” 2019 3rd Cyber Security in Networking Conference (CSNet), 107–113.

[15] Sharma, Rajesh Kumar, and Ravi Singh Pippal. (2020) “Malicious Attack and Intrusion Prevention in IoT Network Using Blockchain Based Security Analysis.” 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 380–385.

[16] Haghighi, Mohammad Sayad, FaezehFarivar, and AlirezaJolfaei. (2020) “A machine learning-based approach to build zero false-positive IPSs for industrial IoT and CPS with a case study on power grids security.” IEEE Transactions on Industry Applications, 1–9.

[17] Kasongo, Sydney Mambwe. (2021) “An advanced intrusion detection system for IIoT based on GA and tree based algorithms.” IEEE Access 9: 113199–113212.

[18] Kumar, Randhir, et al. (2022) “A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network.” Journal of Parallel and Distributed Computing 164: 55–68.

[19] Basati, Amir, and Mohammad Mehdi Faghih. (2022) “PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders.” Information Sciences 598: 57–74

[20] Saheed, YakubKayode, et al. (2022) “A machine learning-based intrusion detection for detecting internet of things network attacks.” Alexandria Engineering Journal 61 (12): 9395–9409.

[21] De Souza, Cristiano Antonio, Carlos Becker Westphall, and Renato Bobsin Machado. (2022) “Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments.” Computers & Electrical Engineering 98: 107694.

[22] A. Derhab, M. Belaoued, M. Guerroumi, and F. A. Khan, “Two-factor mutual authentication offloading for mobile cloud computing,” IEEE Access, vol. 8, pp. 28956–28969, 2020.

[23] A. Boulemtafes, A. Derhab, and Y. Challal, “A review of privacy-preserving techniques for deep learning,” Neurocomputing, vol. 384, pp. 21–45, 2020.

[24] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for internet of things,” Future Generation Computer Systems, vol. 82, pp. 761–768, 2018.

[25] A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues,” Knowledge-Based Systems, vol. 189, article 105124, 2020.

[26] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study,”Journal of Information Security and Applications, vol. 50, article 102419, 2020.

[27] S. Mahdavifar and A. A. Ghorbani, “Application of deep learning to cybersecurity: A survey,” Neurocomputing, vol. 347, pp. 149–176, 2019.

[28] Z. Ning, P. Dong, X. Wang et al., “Mobile edge computing enabled 5g health monitoring for internet of medical things: a decentralized game theoretic approach,” IEEE Journal on Selected Areas in Communications, pp. 1–16, 2020

[29] S. Ni, Q. Qian, and R. Zhang, “Malware identification using visualization images and deep learning,” Computers & Security, vol. 77, pp. 871–885, 2018.

[30] G. Sun and Q. Qian, “Deep learning and visualization for identifying malware familes,” IEEE Transactions on Dependable and Secure Computing, p. 1, 2018.

[31] Y. N. Soe, P. I. Santosa, and R. Hartanto, “Ddos attack detection based on simple ann with smote for iot environment,” in 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1–5, Semarang, Indonesia, 2019.