engineering proceedings

MDPI

Proceeding Paper

An Innovative Intrusion Detection System for High-Density Communication Networks Using Artificial Intelligence †

G. Sirisha [1,*], K. Vimal Kumar Stephen [2], R. Suganya [3], Jyoti Prasad Patra and T. R. Vijaya Lakshmi [5]

[1] Master of Computer Applications, Loyola Academy Degree and PG College, Alwal, Secunderabad, Telangana 500010, India
[2] Department of Information Technology, University of Technology and Applied Sciences, Ibra 400, Oman; vimal.victor@utas.edu.om or vimal@ict.edu.om
[3] Department of Computer Science and Engineering, Dr. N.G.P Institute of Technology, Coimbatore 641048, India; suganrhithu@gmail.com
[4] Department of Electrical and Electronics Engineering, Krupajal Engineering College, Puri Pubasasan Prasanthi Vihar, Bhubanes 751002, India; jpp42003@yahoo.co.in
[5] Department of Electronics and Communication Engineering, Mahatma Gandhi Institute of Technology, Hyderabad 500075, India; trvijayalakshmi_ece@mgit.ac.in
* Correspondence: siriindian99@gmail.com or siribdj.24@gmail.com
† Presented at the International Conference on Recent Advances in Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: The emergence of Machine Learning (ML) strategies within the scope of community security has led to principal advances in improving clever Artificial Intelligence (AI) primarily based on intrusion detection structures. Intrusion Detection Systems (IDSs) are used to locate malicious conduct in conversation systems and the internet. A smart AI-based IDS comprises some additives that enable it to provide an automatic and green safety solutions for high-density verbal exchange structures. Present IDS stumble on intrusions and anomalies that are primarily based on predefined guidelines and signature patterns, whereas clever AI primarily based on IDS uses ML methods to gather significant volumes of information from both external and internal sources to hit upon anomalies that could imply a safety breach. Smart AI-based total IDS combines diverse ML methods which are inclusive of supervised studying, unsupervised learning, deep studying, neural networks, and reinforcement-gaining knowledge to create a holistic security solution.

Keywords: artificial intelligence; network security; intrusion detection; machine learning; high density

Citation: Sirisha, G.; Stephen, K.V.K.; Suganya, R.; Patra, J.P.; Lakshmi, T.R.V. An Innovative Intrusion Detection System for High-Density Communication Networks Using Artificial Intelligence. *Eng. Proc.* **2023**, *59*, 78. https://doi.org/10.3390/engproc2023059078

Academic Editors: Nithesh Naik, Rajiv Selvam, Pavan Hiremath, Suhas Kowshik CS and Ritesh Ramakrishna Bhat

Published: 19 December 2023

1. Introduction

In recent years, the development of high-density communication networks has been accompanied by an immediate need for enhanced intrusion detection systems to mitigate the risks of malicious activities. As such, innovations in intrusion detection technology have become increasingly important [1]. Another important advancement in intrusion detection technology is the application of distributed systems for better network security oversight. By sharing resources across a network of distributed systems, network security specialists have a more comprehensive understanding of activities taking place within a communication network [2]. By developing algorithms that are capable of performing sophisticated statistical analyses, security analysts can quickly identify anomalous behavior within a communication network and identify threats before they can be exploited. The emergence of 5G and IoT technology has also paved the way for improved intrusion detection methods in high-density communication networks. As these technologies continue to permeate our society, the need for improved threat detection capabilities becomes ever more apparent [3]. The recent rapid development of high-density communication networks has necessitated quicker and more accurate intrusion detection solutions. The importance of intrusion detection for high-density communication systems cannot be overstated [4].

High-density communication systems are large networks that consist of high-density transmission elements. By detecting abnormal behavior, such as unauthorized access, data manipulation, denial of service attacks, or probe scans, IDS can quickly alert administrators of any malicious activity [5]. This allows the network administrators to take the necessary steps to protect sensitive data, as well as the system itself, from ongoing attacks. IDS can be used to detect insider threats, which are one of the most difficult threats to address due to the lack of monitoring from the outside [6]. An IDS can be used to detect zero-day attacks, which are attacks that take advantage of vulnerabilities that have not yet been patched. By utilizing artificial intelligence algorithms to identify and analyze patterns of activity, IDS can detect unique and unusual behavior that could indicate if a zero-day attack is taking place [7]. Effective IDS can be used to detect malicious activities from external and internal sources, insider threats, and zero-day attacks, thereby helping to keep data and networks secure. The main contributions of the research are the following:

- Detect unauthorized activities and malicious behavior that pose a risk to the confidentiality, integrity, and availability of network systems and monitor system activity and develop response plans for suspicious events.
- Enable faster responses to detected threats by providing real-time threat detection and strengthen the overall security posture of a network system by providing additional layers of defense.
- Identify potential weaknesses in the system by pinpointing the ways attackers may take advantage of vulnerabilities and streamline the process of detecting and responding to security events, thereby reducing response time [8–10].

2. Materials and Methods

The use of high-density communications systems has seen immense growth over the past few years. These systems, which are heavily dependent on short-range wireless networks, are especially popular in heavily populated areas and in places where large numbers of people congregate, such as airports, stadiums, and shopping malls. High-density network challenges prompting AI-based IDS can include:

- Identifying suspicious connections to detect potential malicious attacks.
- Detecting multiple types of attacks, including known attacks, zero-day attacks, advanced persistent threats, and targeted attacks.
- Producing real-time alerts for responses within a few seconds.

2.1. Related Works

This makes the need for intrusion detection and protection of these high-density communications systems essential [11]. Intrusion detection is critical for high-density communications systems because the large number of devices and users makes it easier for malicious actors to gain access and take advantage of weak points in the system [12]. The challenge of intrusion detection in high-density communications systems can be addressed with the use of big data analytics and machine learning algorithms [13]. In addition to the use of big data analytics and machine learning algorithms, the security of high-density communications systems can be further strengthened with the use of encryption and authentication methods. Encryption can prevent data interception and alteration, while authentication can be used to control who has access to the network and the data they can access. It is difficult to detect malicious attacks targeting high-density communications systems due to their complexity [14]. With highly interconnected communication networks, it can be difficult to detect sophisticated attacks and malicious activity hidden in the vast amounts of user traffic [15]. Multi-hop communication networks provide a greater level of obfuscation, making it easier for attackers to hide their malicious activities in normal user traffic. Furthermore, it can be difficult to accurately monitor large amounts of network traffic in real-time since intrusion detection systems require extensive resources and computational power to process the network traffic [16]. As such, it is important to employ more advanced techniques such as anomaly-based detection methods to detect malicious

activities. Due to the complicated structure of high-density communication systems, the implementation of intrusion detection systems can be complex and costly [17]. Additionally, organizations should implement comprehensive logging systems to better track and record any suspicious activity. The intrusion detection in high-density communication systems remains an arduous task for security professionals [18]. Although implementing such systems can be challenging and costly, the safety of communication networks should be taken seriously and organizations should prioritize the security of our digital infrastructure. The novel AI-Based Intrusion Detection System (IDS) for high-density communication systems uses an innovative combination of machine learning algorithms and deep learning techniques to detect and identify malicious behavior in communications data [19]. By using artificial intelligence and deep learning models, the system can identify new emerging trends in malicious behavior that may otherwise be difficult to detect [20].

2.2. Proposed Model

An AI-based Intrusion Detection System (IDS) for high-density communication systems refers to a system that uses Artificial Intelligence (AI) techniques to detect abnormal behaviors or malicious attacks in a highly dense network. A financial services provider has deployed AI-driven IDS to monitor its digital assets and protect them from malicious attacks. The IDS uses a combination of Natural Language Processing (NLP), fuzzy logic, and machine learning algorithms to detect potential malicious activities. When an activity is detected, the IDS send an alert to the security team to investigate.

$$\left(\frac{i * i_m}{n_m}\right) = \frac{1}{2} i * n_m^2 \tag{1}$$

The purpose of the following is to provide an overview of the construction of an Artificial Intelligence (AI)-based intrusion detection system for high-density communication systems:

$$n_m^2 = \left(\frac{i * i_m}{n_m}\right) * \frac{2}{i} \tag{2}$$

It will discuss the advantages and disadvantages of this type of system. The first aspect of construction of an AI-based IDS for high-density communication systems is the model used for learning:

$$n_m^2 = \left(\frac{2 * i_m}{n_m}\right) \tag{3}$$

Deep learning models can be trained to detect patterns in data streams and identify intrusion attempts faster than traditional models by utilizing multiple layers of processing:

$$o = \left(\frac{i_m}{n_m^2}\right); \tag{4}$$

Furthermore, the construction of an AI-based IDS for high-density communication systems must include a variety of security related tools:

$$n_m^2 = 2 * n * n_m \tag{5}$$

Additionally, the utilization of high-speed, high-density network interfaces allows for rapid communication with and between network devices:

$$n_m = \sqrt{2 * n * i_m} \tag{6}$$

Additionally, due to the sophisticated nature of the AI model, there is also a potential for the model to make incorrect decisions, leading to false positives and network disruptions:

$$o\prime(m) = \lim_{n \to 0} \left(\frac{o(m+n) - o(m)}{n} \right) \tag{7}$$

As such, it is important to consider the various components, tools, and models necessary for an effective and secure system. An AI-based intrusion detection system (IDS) is a security system that uses artificial intelligence algorithms to detect malicious activities or data unauthorized access to computer networks. The functional block diagram has shown in the following Figure 1.

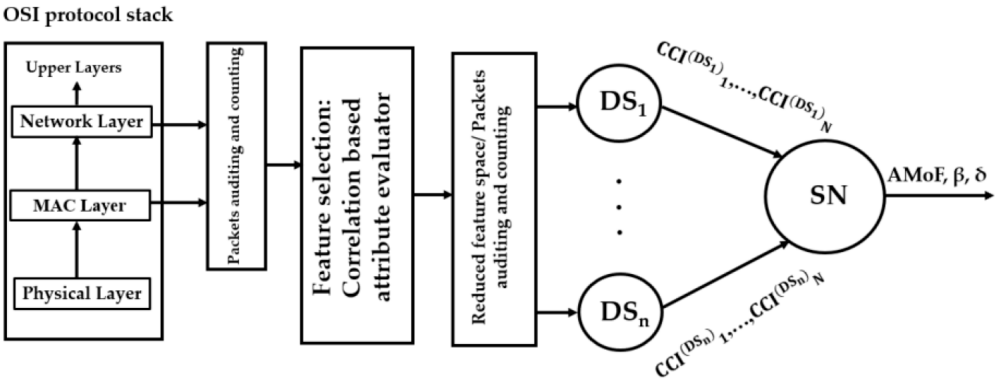

Figure 1. Functional block diagram.

These models are trained on malicious and benign data samples to differentiate between malicious and normal activities:

$$o\prime(m) = \lim_{n \to 0} \left(\frac{o^{m+n} - o^{m}}{n} \right) \tag{8}$$

The main purpose of these systems is to detect anomalies in data or user behavior that could indicate an attack. An AI-based intrusion detection system for a high-density communication system is designed to secure the system against potential threats:

$$o\prime(m) = \lim_{n \to 0} \left(\frac{(o^{m} * o^{n}) - o^{m}}{n} \right) \tag{9}$$

It is most useful in systems that handle a large volume of data. The AI-based intrusion detection system works by analyzing incoming data packets to detect suspicious activities. It can detect attacks such as malware, buffer overflows, obscure injections, etc.:

- Robust detection: AI-backed real-time anomaly detection can identify malicious activity very precisely in high-density networks. It can differentiate between innocuous and malicious traffic so accuracy is ensured.
- Automated monitoring: The AI-powered anomaly detection system is automated and constantly monitors network traffic to detect any malicious activity. This helps to mitigate threats quickly.
- Scalability: The system can be easily scaled up and down to accommodate networks of different sizes and densities, making it an excellent choice for high-density networks.

Furthermore, the needs of the environment should be assessed. Before integrating AI-based IDS into a network infrastructure, it is important to assess the current needs of the environment. This includes analyzing the size of the network, the types of traffic, the purpose of the network, and the level of security required. The operational flow diagram has shown in the following Figure 2.

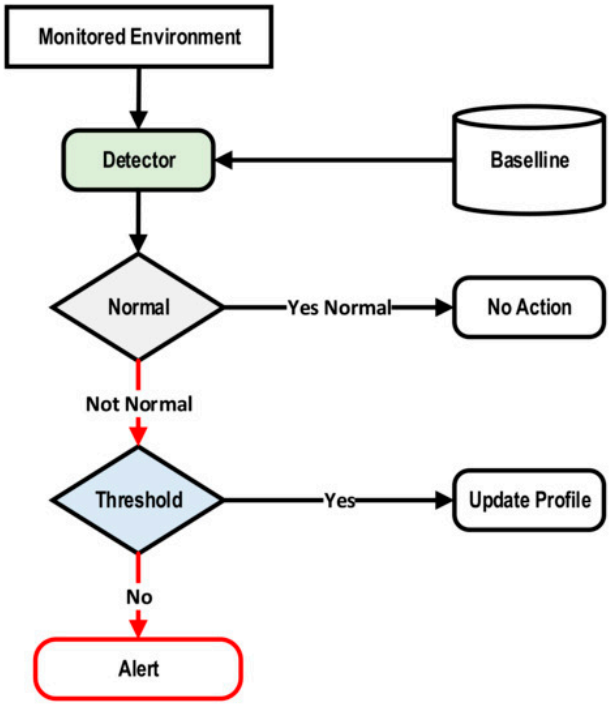

Figure 2. Operational flow diagram.

Additionally, it can also be trained to detect the evolution of cyber threats and adjust its defenses appropriately. The AI-based intrusion detection system makes use of techniques such as deep learning and machine learning to detect anomalies accurately:

$$o''(m) = e^m * \lim_{n \to 0} \left(\frac{1 - e^n}{n} \right) \tag{10}$$

It can be used to monitor various components in a high-density communication network, such as routers, hubs, switches, and firewalls.

3. Results and Discussion

The proposed AI-based Intrusion Detection System (AIIDS) is compared with the existing Lightweight Intelligent Intrusion Detection System (LIIDS), Intrusion Detection System (IDS), Intelligent Intrusion Detection System (IIDS), and LSTM-Based Intrusion Detection System (LIDS). Here, the network simulator (NS-2) has the simulation tool used to execute the results.

AI-based intrusion detection systems must be able to accurately detect even the most subtle of threats as well as distinguish between benign and malicious activities with a high degree of accuracy.

Figure 3 shows the computation of miss rate. In a comparison cycle, the existing LIIDS obtained 64.94%, IDS reached 58.28%, IIDS secured 66.83%, and LIDS scored 56.87% miss rate. The proposed AIIDS reached 87.00% miss rate.

In AI-based intrusion detection systems for high-density communication systems, the computation of false alarm (or false positive) rate is an important metric of the overall performance of the system. Figure 4 shows the computation of fall out. In a comparison cycle, the existing LIIDS obtained 74.94%, IDS reached 68.28%, IIDS secured 76.83%, and LIDS scored 66.87% fall out. The proposed AIIDS reached 87.00% fall out. Prevalence is a measure of how often a given pattern or anomaly is found within a particular data set. In AI-based intrusion detection systems, prevalence is a measure of how likely it is that an attack will occur.

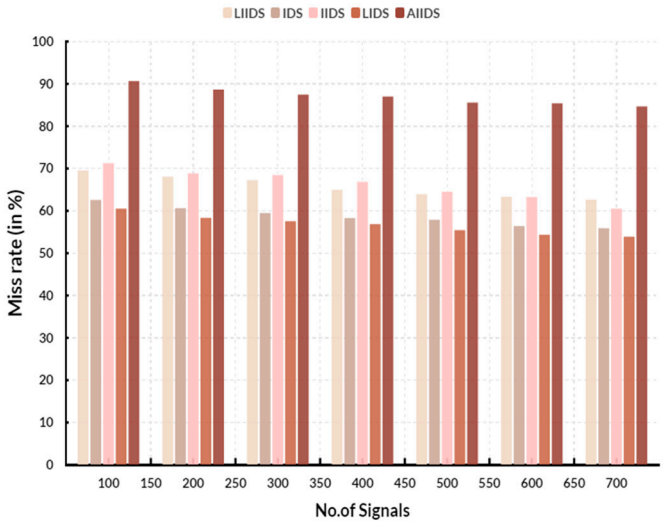

Figure 3. Miss rate.

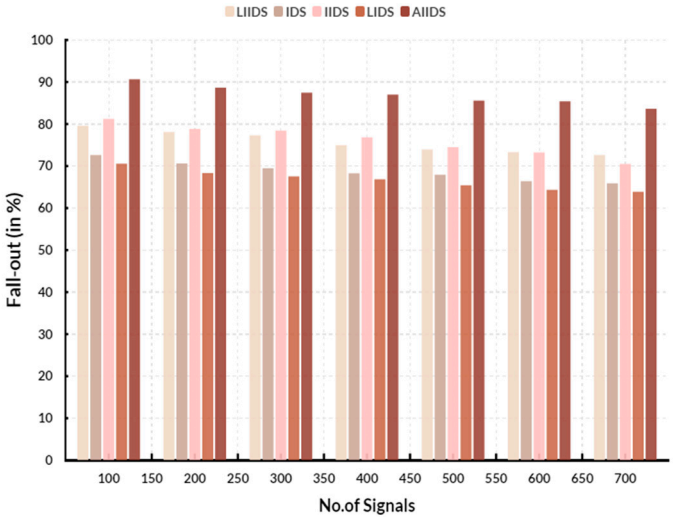

Figure 4. Fallout.

Figure 5 shows the computation of prevalence. In a comparison cycle, the existing LIIDS obtained 66.77%, IDS reached 61.50%, IIDS secured 78.61%, and LIDS scored 61.65% prevalence. The proposed AIIDS reached 80.96% prevalence. The challenges related to interpretability and generalizability of constituents is as follows:

- A lack of accuracy and robustness of outcomes when presented with new datasets and tasks.
- Limited access to data gathering (from human experts or external sources) and verification processes.
- Low scalability due to architectural constraints and hardware requirements.

System scalability refers to the ability of a system to expand or contract in size and complexity as demand increases or decreases. Scalability is important, considering that network traffic is ever-changing, and organizations need to be able to respond quickly and efficiently to changes. Scalability helps to ensure that a system can be easily upgraded or downgraded to meet the needs of the organization.

Compatibility refers to the ability for a system to communicate and work with other systems. Compatibility is important in order to ensure that all components of a system can work together without any problems. In order to ensure complete compatibility, it is important to consider possible changes that could occur in the future, as well as the types of hardware and software that could be used in the system:

- Explainability: Explainability measures enable the identification of easily understandable rules or features underlying a system's decision. Visualizations, such as heat maps of important features, can be used to provide context and explain the rationale behind an AI system's decisions.
- Transparency: Transparency aims to provide an insight into the underlying data or training process that has produced the AI system. This can be performed by providing access to logs, training datasets, and algorithm codes.
- Trustworthiness: Measures such as audits and tests can be used to establish trust in the decisions made by the AI-driven IDS. This includes ensuring that the system operates according to intended parameters, such as fairness or accuracy.

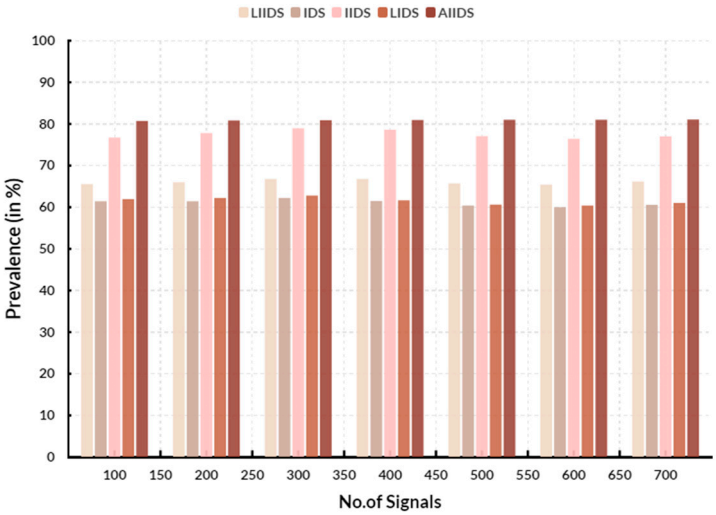

Figure 5. Prevalence.

The potential cost-effectiveness of using an IDS compared to traditional IDS depends on the size of the organization and the amount of traffic that the system needs to monitor. IDS systems can be relatively expensive compared to traditional security measures, but their ability to detect and respond to security incidents makes them a cost-effective investment. Additionally, IDS systems can provide additional protection with minimal impact on network performance.

4. Conclusions

AI-based intrusion detection systems have a large potential to become a core component of high-density communication systems. They can be used to monitor and detect suspicious activities in real-time, thus preventing any malicious activity from taking place. By using Machine Learning (ML) and Artificial Neural Networks (ANNs), systems can be trained to detect intrusions based on specific patterns or certain behaviors. AI-based systems could also learn from historical data and find anomalies that indicate an attack is underway. These systems could then be used to create more accurate alerts that inform systems administrators of any suspicious activity. Additionally, AI-based intrusion detection systems could be implemented to protect user data, such as when storing customer information on distributed databases. AI technologies can detect data breaches and protect the data from malicious attacks or unauthorized access. An active network monitoring is an important tool that can help to strengthen network security guidelines by suppressing malicious activities. Through intelligent active monitoring of interfaces, network administrators can gain real-time understanding of the health of the network and identify malicious behaviors in order to avoid harmful attacks. In addition, active monitoring can be used to investigate security incidents and return networks to their normal state.

Author Contributions: Conceptualization, G.S. and K.V.K.S.; methodology, R.S.; software, J.P.P.; validation, J.P.P., R.S. and T.R.V.L.; formal analysis, T.R.V.L.; investigation, R.S.; resources, T.R.V.L.; data curation, T.R.V.L.; writing—original draft preparation, K.V.K.S.; writing—review and editing, G.S.; visualization, J.P.P.; supervision, K.V.K.S.; project administration, K.V.K.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Whelan, J.; Almehmadi, A.; El-Khatib, K. Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. *Comput. Electr. Eng.* **2022**, *99*, 107784. [CrossRef]
2. Salman, E.H.; Taher, M.A.; Hammadi, Y.I.; Mahmood, O.A.; Muthanna, A.; Koucheryavy, A. An Anomaly Intrusion Detection for High-Density Internet of Things Wireless Communication Network Based Deep Learning Algorithms. *Sensors* **2022**, *23*, 206. [CrossRef] [PubMed]
3. Mendonca, R.V.; Silva, J.C.; Rosa, R.L.; Saadi, M.; Rodriguez, D.Z.; Farouk, A. A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. *Expert Syst.* **2022**, *39*, e12917. [CrossRef]
4. Yadav, N.; Pande, S.; Khamparia, A.; Gupta, D. Intrusion detection system on IoT with 5G network using deep learning. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9304689. [CrossRef]
5. Muthanna, M.S.A.; Alkanhel, R.; Muthanna, A.; Rafiq, A.; Abdullah, W.A.M. Towards SDN-enabled, intelligent intrusion detection system for internet of things (IoT). *IEEE Access* **2022**, *10*, 22756–22768. [CrossRef]
6. Imanbayev, A.; Tynymbayev, S.; Odarchenko, R.; Gnatyuk, S.; Berdibayev, R.; Baikenov, A.; Kaniyeva, N. Research of machine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond. *Sensors* **2022**, *22*, 9957. [CrossRef] [PubMed]
7. Yu, Y.; Zeng, X.; Xue, X.; Ma, J. LSTM-based intrusion detection system for VANETs: A time series classification approach to false message detection. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 23906–23918. [CrossRef]
8. Amanoul, S.V.; Abdulazeez, A.M. Intrusion detection system based on machine learning algorithms: A review. In Proceedings of the 2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA), Selangor, Malaysia, 12 May 2022.
9. Shitharth, S.; Kshirsagar, P.R.; Balachandran, P.K.; Alyoubi, K.H.; Khadidos, A.O. An innovative perceptual pigeon galvanized optimization (PPGO) based likelihood Naïve Bayes (LNB) classification approach for network intrusion detection system. *IEEE Access* **2022**, *10*, 46424–46441. [CrossRef]
10. Onyema, E.M.; Dalal, S.; Romero, C.A.T.; Seth, B.; Young, P.; Wajid, M.A. Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities. *J. Cloud Comput.* **2022**, *11*, 26. [CrossRef]
11. Alani, M.M.; Awad, A.I. An Intelligent Two-Layer Intrusion Detection System for the Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *19*, 683–692. [CrossRef]
12. Park, C.; Lee, J.; Kim, Y.; Park, J.G.; Kim, H.; Hong, D. An enhanced AI-based network intrusion detection system using generative adversarial networks. *IEEE Internet Things J.* **2022**, *10*, 2330–2345. [CrossRef]
13. Rizvi, S.; Scanlon, M.; McGibney, J.; Sheppard, J. Deep learning based network intrusion detection system for resource-constrained environments. In Proceedings of the International Conference on Digital Forensics and Cyber Crime, Boston, MA, USA, 16–18 November 2022; Springer Nature: Cham, Switzerland, 2022; pp. 355–367.
14. Ragab, M.; Sabir, M.F.S. Outlier detection with optimal hybrid deep learning enabled intrusion detection system for ubiquitous and smart environment. *Sustain. Energy Technol. Assess.* **2022**, *52*, 102311. [CrossRef]
15. Friha, O.; Ferrag, M.A.; Shu, L.; Maglaras, L.; Choo, K.K.R.; Nafaa, M. FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things. *J. Parallel Distrib. Comput.* **2022**, *165*, 17–31. [CrossRef]
16. Hnamte, V.; Hussain, J. DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telemat. Inform. Rep.* **2023**, *10*, 100053. [CrossRef]
17. Tang, F.; Chen, X.; Zhao, M.; Kato, N. The Roadmap of Communication and Networking in 6G for the Metaverse. *IEEE Wirel. Commun.* **2022**, *30*, 72–81. [CrossRef]
18. Saheed, Y.K.; Abiodun, A.I.; Misra, S.; Holone, M.K.; Colomo-Palacios, R. A machine learning-based intrusion detection for detecting internet of things network attacks. *Alex. Eng. J.* **2022**, *61*, 9395–9409. [CrossRef]

19. Chang, V.; Golightly, L.; Modesti, P.; Xu, Q.A.; Doan, L.M.T.; Hall, K.; Kobusińska, A. A survey on intrusion detection systems for fog and cloud computing. *Future Internet* **2022**, *14*, 89. [CrossRef]
20. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]