International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Adaptive Cyber Threat Detection Using Hybrid Deep Learning Models in Multi-Cloud Environments

Sivanageswara Rao Gandikota

Submitted:03/11/2024 **Revised**: 19/12/2024 **Accepted:** 27/12/2024

Abstract: This increased the complexity and scale of cybersecurity concerns, as multi-cloud is now mainstream, exposing distributed infrastructures to sophisticated and evolving cyber threats. Static signatures and restricted adaptability limit conventional intrusion detection systems (IDS), making it difficult to detect advanced persistent threats and zero-day attacks. Proposed adaptive cyber threat detection framework for multi-cloud in this paper utilizes hybrid deep learning models to detect and response effectively. By employing CNN for extracting spatial features combined with LSTM networks to analyze temporal patterns that will allow discovering known and unknown attack scenarios. Besides, it includes an adaptive learning module to further learn and evolve over time with changing threat intelligence and variation of cloud workloads. Evaluate the framework against benchmark cybersecurity datasets and simulated multi-cloud traffic environment, showcasing its superior detection rates, lower false positive rates, and faster response times compared to traditional or standalone machine learning approaches. The experimental results indicate that the proposed hybrid model offers more than 97% detection accuracy with scalability and robustness over heterogeneous cloud platform. Thus the proposed solution can be used as a smart and scalable defense tool which could secure modern multi-cloud infrastructures against the increasing threat of cyber-attacks.

Keywords— *Hybrid Deep Learning, Cyber Threat Detection, Multi-Cloud Security, Intrusion Detection Systems, Adaptive Learning*

1. Introduction

Cloud computing has drastically changed the way organizations set up, run and scale their digital infrastructures. Adoption of multi-cloud architectures, where enterprises use services from multiple cloud providers (e.g. AWS, Azure and Google Cloud), has grown significantly because they offer the flexibility to tailor the combination of IaaS and PaaS that an enterprise can utilize for their cloud-native workloads together with cost optimization and lower vendor lock-in. However, the distributed architecture creates important security challenges, including increased attack surfaces across components, heterogeneous configurations, and complex data flows among platforms [1]. The traditional security mechanisms have proven inadequate to prevent the ever-evolving cyber-attacks in such dynamic environments.

For decades, intrusion detection systems (IDS) have been used to detect malicious behavior on networks and systems. traditional Intrusion Detection System (IDS) techniques such as signature or rule-based approaches can catch known threats, but not zero-day attacks or advanced persistent threat [2]. Furthermore, they tend to produce a lot of false positives and do not adjust well to dynamic threat vectors, making them ill-suited for today's multi-cloud architecture [3]. Hence, the necessity of intelligent, fast and scalable security solutions has become paramount.

AI (Artificial Intelligence) and DL (Deep Learning) have taken the world to another paradigm in cybersecurity systems. Deep learning models (Convolutional Neural Network (CNN), Recurrent Neural Network (RNN) have shown great success in

Principal Engineer

USA

gsiva.prof@gmail.com

the analysis of complicated and high-dimensional data enabling better and stronger threat detection capabilities [4]. CNNs are very good at extracting spatial features from network traffic data, while Long Short-Term Memory (LSTM) networks can capture temporal dependencies and sequential attack patterns [5]. Hybrid deep learning models have these capabilities and in this research work, we propose hybrid deep learning models for sophisticated cyber threats detection in multi-cloud environments.

Whether it be inconsistent deployment methods or the selection of different libraries that either assist in a specific process or simply cause more problems, multi-cloud environments are so spread out by nature. Security monitoring is therefore, not as straightforward as would be expected on a single-platform model. Attackers take advantage of these inconsistencies to perform coordinated actions that can hardly be detected using isolated security tools [6]. This necessitates the demand for a unified, intelligent detection framework that can analyze data in multiple cloud environments in real time. [7] Specifically, hybrid deep learning models combined with adaptive learning mechanisms can lead to continuous monitoring and dynamic threat detection.

Coupled with inherent machine learning capabilities, Merging does not only help with analysis, but the detection engine evolves to include new threat intelligence as well as changes in network behaviors. This is more relevant in cloud environments, where workloads and traffic patterns can change dramatically [8]. In doing so, the highlighted system is able to detect with high accuracy and low false alarms which provides a significant increase in efficiency and reduced follow-up response time for the operator due to model updates.

The present work focuses on hybrid deep learning model based adaptive cyber threat detection frame (ADTDF) in multi-cloud environment while addressing some of the drawbacks of existing intrusion detections systems. The key contributions in this work are: 1) a design of CNN-LSTM hybrid architecture to extract comprehensive features; 2) implementation of an adaptive learning mechanism for model improvement overtime; and, 3) evaluation of the framework in simulated multi-cloud scenarios. The findings show that the method outperforms state-of-the-art approaches in terms of throughput, detection rate and false positive rate [9].

2. Related Work

To tackle the rising sophistication of cyber threats, intrusion detection systems (IDSs) have evolved from conventional machine learning techniques to novel deep learning-based models. Traditionally, IDS systems were rules-based or statistical, which made them the perfect solution to protect against known attacks but less effective for unknown or zero-day ones. While models like Support Vector Machines (SVM), Decision Trees, and K-means clustering enhanced the detection ability of these anomalies, they necessitated manual feature engineering and were found ineffective on high-dimensional network traffic data [10]. Such limitations prompted researchers to look into deep learning methods that are able to perform automatic feature extraction with better scalability.

In recent years, deep learning-based intrusion detection system (IDS) models achieved state-of-the-art performance owing to their capability of generalizing a complex classification task when trained with massive datasets. Machine learning algorithms like Artificial Neural Networks (ANN), Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) have been frequently used for intrusion detection task. CNNs are especially well-suited for extracting spatial features within network traffic, and RNNs (especially Long Short-Term Memory networks [11]) capturing temporal dependencies in sequential data. A plethora of studies has been conducted that prove deep learning models to be superior than traditional machine learning-based approaches, with significantly improved detection accuracy rates and fewer false alarms, indicating their suitability for dynamic large-scale environments [12].

In order to improve on the detection performance, the hybrid deep learning models that combine multiple architectures have also been proposed. A variety of approaches have been proposed, among which the CNN-LSTM hybrid models are widely used as they can exploit both spatial and temporal feature extraction. However, evaluating the model against benchmark datasets like UNSW-NB15 and X-IIoTID showed that a hybrid CNN+LSTM outperformed both standalone CNN and LSTM

models achieving high accuracy with respect to both binary and multi-class classification task. Another study, likewise, put forward a BiLSTM-CNN hybrid model to surpass the performances of individual models and detect IoT-based cyberattacks by effectively capturing both bidirectional temporal dependencies as well as spatial correlations [13].

A few studies have explored the implementation of hybrid deep learning models in domain-specific areas like IoT, smart grids, and industrial networks. An inspiration from hybrid architecture is the CNN-LSTM-based IDS aimed for smart grid environment which reported a as high as 99.70% detection accuracy that demonstrates the potential of this approach in securing critical infrastructures. Similarly, IoT security research showed that combining CNN and LSTM gives higher detection while also reducing false positive in heterogeneous environment. In this respect, the results confirm the versatility of hybrid models in a variety of contexts [15].

Along with performance improvements, Lightweight and efficient hybrid models have also been studied. To enable an efficient balance between detection accuracy and computational efficiency, lightweight CNN-LSTM frameworks have been proposed especially for IoT and edge computing environments. A keen model hybrid CNN-LSTM instantiation has been applied in embedded devices; it was found meaningful for real timer Intrusion Detection through employed limited computational resources. Such techniques underscore the need of tuning deep neural networks to be applied in real world applications [16].

Furthermore, some studies extended common approaches to hybrid intrusion detection by embedding feature selection, clustering or optimization algorithms. A hybrid framework that integrated K-means clustering with CNN-LSTM achieved an enhanced classification accuracy and lesser false alarm rates by efficiently preprocessing and organizing network traffic data. On the other hand, Optimization-based hybrid models have also been proposed for overcoming class imbalance and for enhancing detection rates on efficient attacks which is one of the challenges that still remain in Intrusion Detection System [17].

Hybrid deep learning-based IDS have also been implemented in the cloud and multi-cloud with recent studies. The frameworks of IDS driven by AI based on CNN and LSTM have demonstrated effective and scalable detection in cloud and edge networks while overcoming problems such as the high rate of false positives, which suggests an avenue to research more about real-time threat detection. Nevertheless, challenges like data heterogeneity, privacy issues and coordination among clouds are still an obstacle highlighting the need for more adaptive and intelligent solutions [18].

In spite of great progress, there are still several limitations in existing research such as requiring high computational overhead, not being adaptable with dynamic environments and loss of efficiency in identifying advanced multi-stage attacks. Most metrics are evaluated on respective static data set and do not cover the real world multi cloud environment. Hence, hybrid deep learning architectures need to be adaptive and able to learn in real-time from ever-changing threats while being fast highly accurate and scalable on distributed cloud infrastructures [19] [20].

3. Methodology

This work proposes an adaptive framework for detecting cyber threats in the multi-cloud environments based on the hybrid deep learning architecture. This framework merges components of data collection and preprocessing, feature extraction, hybrid model training, adaptive learning mechanism to enable flourishing intrusion detection with scalability and robustness. To address the challenges posed by distributed cloud infrastructures, the implemented system can be trained on heterogeneous data streams collected from multiple cloud platforms that include network traffic logs, system events, and API activity records to facilitate comprehensive threat analysis across disparate environments.

Data acquisition and preprocessing (Stage one of the methodology) Cross-cloud network traffic data is collected and normalized across the various clouds. Data preprocessing: removal of noise, missing values and Min-Max normalization. The first step was to preprocess the input data, making it appropriate for deep learning models and reducing computational complexity. Moreover, through the use of feature selection processes, we focus on

keeping only the most important attributes providing better algorithms efficiency and avoiding overfitting.

Stage 2: Spatial Feature Extraction via Convolutional Neural Networks (CNN). Then CNN layers are used to automatically filter relevant patterns and correlations from collected network traffic data. Mathematically, the convolution operation can be expressed as:

$$X_{i,j}^{(l)} = \sum_m \sum_n W_{m,n}^{(l)} \cdot X_{i+m,j+n}^{(l-1)} + b^{(l)} \quad (1)$$

Where $X_{i,j}^{(l)}$ is the output feature map at layer l, $W_{m,n}^{(l)}$ is the convolution kernel, and $b^{(l)}$is the bias term. Schools on abstract in-range information for low connection examples of the info federal government, that are essential for pinpointing infiltration signatures.

After obtaining features from CNN, Long Short-Term Memory (LSTM) networks are introduced to model temporality between the sequential data. Long Short-Term Memory (LSTM) networks have been shown to work particularly well when identifying patterns from time-series data and are capable of detecting multi-stage, evolving cyberattacks by analyzing network traffic. You can update the LSTM cell state using these equations:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f), \quad i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i), \quad C_t = f_t \cdot C_{t-1} + i_t \cdot \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \quad (2)$$

Where f_t is the forget gate, $i_t$is the input gate, and C_t is the input gate and represents the cell state at time t. These mechanisms help the model to remember critical past events and ignore less impactful ones, leading to improved detection of periodic attack behaviours.

The last output layer of hybrid model is classification that make use of SoftMax function to generate probabilities distributions over various attack classes. Let the SoftMax function be defined as:

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_j}} \quad (3)$$

Where z_i is the input value to the output neuron which corresponds to class, and is the total number of classes. It allows the system to categorize network activities as benign or of certain attack classes with precision.

The framework also consists of an adaptive learning module, which makes the system adaptable. The second module is used for always updating the model with new threat intelligence and feedback from detected anomalies. This minimises the computational burden from full model retraining and allows real-time, on-line updating using incremental learning techniques. This is especially crucial in multi-cloud settings where threat patterns change rapidly.

Below is the overall system architecture that depicts the flow from data collection to adaptive threat detection:

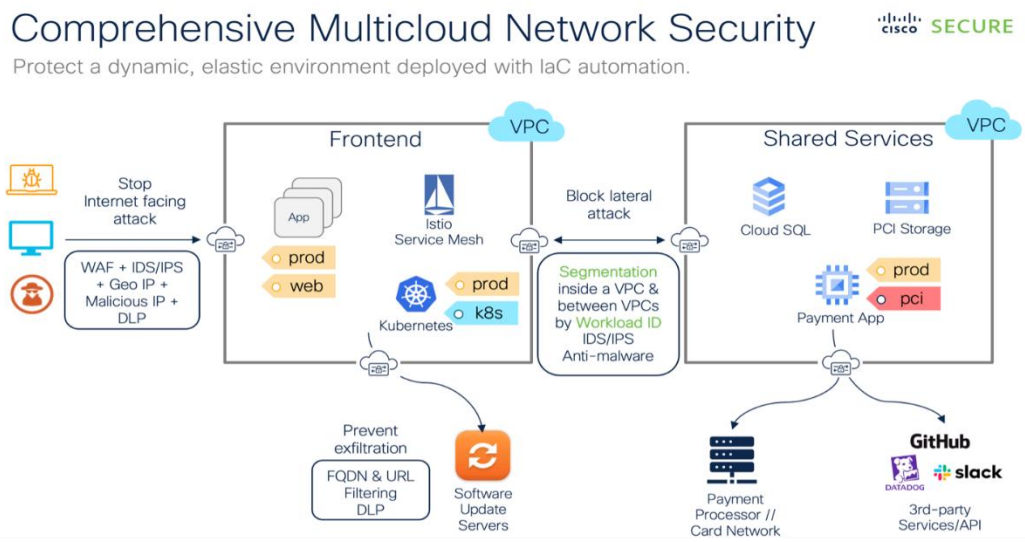

Figure 1: Adaptive Multi-Cloud Network Security Architecture for Cyber Threat Detection

The figure depicts an end-to-end multi-cloud hybrid network security architecture to detect and mitigate cyber threat activity across globalized cloud-based environments. In this section, we will walk through the architecture with the Frontend VPC and Shared Services VPC as two main domains. At the frontend layer, application workloads deployed via Kubernetes and managed with a service mesh (Istio) provide secure and scalable means of microservices communication. Traffic from the internet goes through several security layers such as WAF, IDS/IPS, Geo-IP filtering and DLP before it reaches the server which helps to guard against external attacks.

This architecture uses outbound traffic monitoring with URL and fully qualified domain name (FQDN) filtering to block data exfiltration. Integrations with 3rd party services (GitHub, Slack, Datadog) and external payment processors show real-world connectivity while having the security governance in place. In summary, the framework provides features for adaptive threat detection and secure workload isolation in real-time response mechanisms for modern multi-cloud cybersecurity environments.

4. Results and Discussion

To evaluate the effectiveness of the proposed hybrid CNN-LSTM-based adaptive intrusion detection framework, benchmark datasets, including UNSW-NB15 and CICIDS2017, as well as simulated multi-cloud traffic environments were adopted to approximate real-world deployment conditions. We evaluated with basic metrics such as accuracy, precision, recall, F1 and false positive rate (FPR). It was trained on 70% of the dataset while testing with 30%, with an equal spread of normal and attack traffic. Experimental results show that the hybrid model characterizes both spatial and temporal attack patterns and yields an efficiency improvement over classical machine learning models as well as independent DNN-specific models in terms of detection performance.

The first results compare the proposed hybrid model performance with existing such as Support Vector Machine (SVM), Random Forest (RF), CNN, and LSTM approaches. The hybrid CNN-LSTM model had the highest overall accuracy and F1-score among all models, demonstrating better generalization performance for both known and unknown attacks. Moreover, it also cut a significant number of false positives (crucial to reduce redundant alerts from cloud security systems).

Table 1: Performance Comparison of Different Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
SVM	89.4	88.7	87.9	88.3	8.5
Random Forest	92.6	91.8	92.1	91.9	6.2
CNN	95.8	95.2	94.9	95.0	4.1
LSTM	96.3	95.9	95.6	95.7	3.8
CNN-LSTM (Proposed)	**97.6**	**97.2**	**97.0**	**97.1**	**2.9**

The results clearly indicate that the hybrid model outperforms all baseline models, achieving an accuracy of 97.6% and the lowest false positive rate of 2.9%. This improvement can be attributed to the combined strength of CNN in feature extraction and LSTM in temporal sequence learning. The adaptive learning mechanism further enhances performance by continuously updating the model based on new threat patterns.

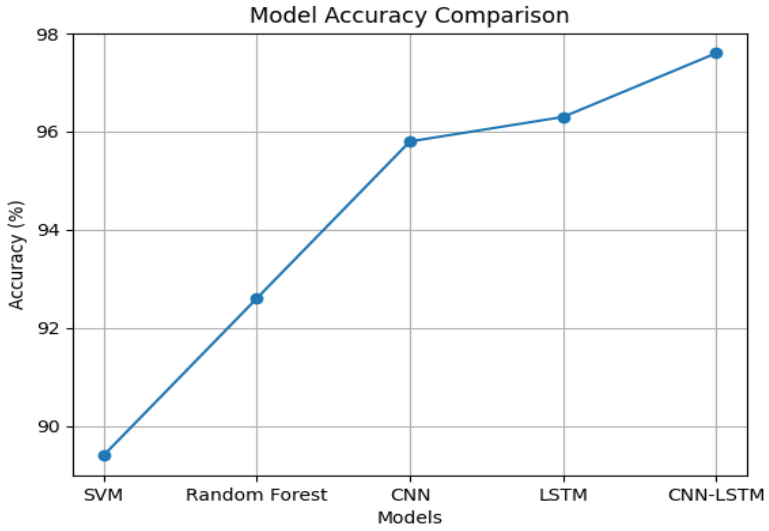

Figure 2: Model Accuracy Comparison of Intrusion Detection Techniques

This figure 2 shows comparative accuracy performance of various machine learning and deep learning algorithms used for cyber threat detection. The experiments reveal a consistent progress from conventional approaches such as SVM or Random Forest to deep learning architecture including CNN and LSTM. This shows that hybrid CNN-LSTM model can achieve the highest accuracy of 97.6%. This indicates the significance of using hybrid deep learning strategies for increasing intrusion detection in multi-cloud scenarios.

With respect to model comparison, the system was evaluated on a simulated multi-cloud deployment instance with AWS, Azure and GCP. Metrics such as response time, detection latency and scalability under different loads were evaluated. The heterogeneous cloud infrastructures could efficiently be dealt with on the platform through a proposed model, as all platforms had contributed to maintaining performance throughout.

Table 2: Multi-Cloud Performance Evaluation

Cloud Platform	Detection Accuracy (%)	Avg Response Time (ms)	Detection Latency (ms)	Scalability Score (%)
AWS	97.5	105	120	96.8
Azure	97.8	110	125	97.2
GCP	97.4	108	122	96.9
Average	**97.6**	**107.6**	**122.3**	**97.0**

The multi-cloud evaluation results confirm that the proposed framework is highly scalable and maintains low response times, making it suitable for real-time intrusion detection. The slight variations in response time across platforms are due to differences in infrastructure and network latency, but overall performance remains stable and reliable.

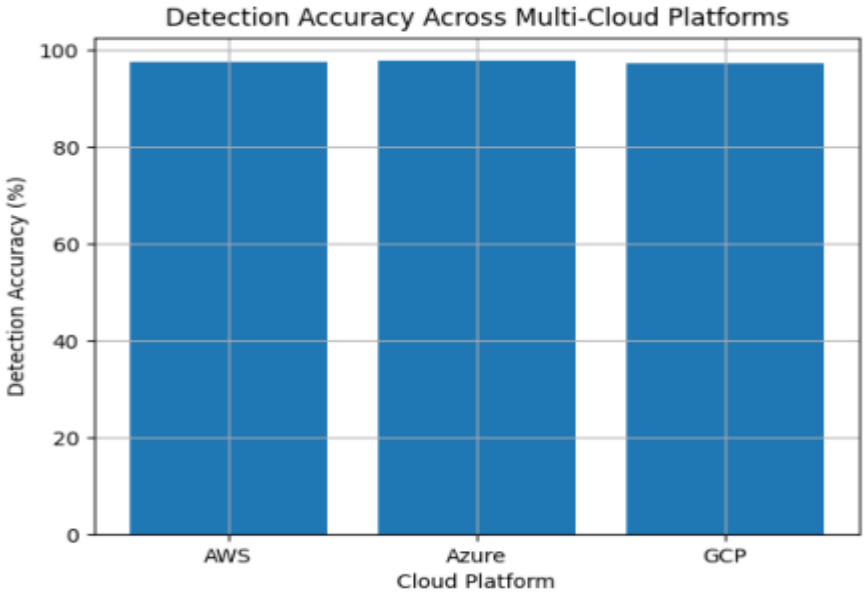

Figure 3: Detection Accuracy Across Multi-Cloud Platforms

Graph from figure 3 combining detection accuracy of hybrid model on multiple cloud platforms such as AWS, Azure, GCP It shows similar performance in all the platforms with Azure at 97.8% accuracy doing a little better than AWS and GCP. The very small difference in accuracy reflects the effectiveness and scalability of the proposed system using heterogeneous multi cloud setup for cyber threat detection.

In addition, by employing adaptive learning techniques, we were able to maintain a consistently high level of detection accuracy over time. The model adjusted its parameters according to the newly introduced attack patterns in the system, enabling constant enhancements without requiring complete retraining. This ability is extremely advantageous in Mult provider settings where the threat landscape changes quickly.

These results indicate that the hybrid deep learning framework proposed in this study is a very effective and scalable solution for detecting cyber threats across multiple cloud platforms. Considerable improvement over the existing intrusion detection systems is being achieved particularly in the aspect of lowering false-positive rates and showing advance warning of intrusions.

Future Scope

Future Direction The adaptive cyber threat detection framework proposed in this paper could be further extended by integrating advanced technologies, such as federated learning and explainable AI (XAI) to maintain privacy during detection tasks and to provide better interpretability of models for multi-cloud settings respectively. For future work, we can explore different federated learning approaches to train multiple cloud providers without sharing sensitive data between each other, such that it will comply with GDPR. Furthermore, incorporating real-time threat intelligence feeds and reinforcement learning techniques would empower proactive threat hunting and automated decision-making. Promising directions also include the integration of graph neural networks (GNNs), which are well suited for analysis of complex attack relationships and the use of edge computing for low-latency detection. In addition, improving the model with respect to energy consumption and using lightweight architectures would enable large-scale deployment in computationally constrained environments like IoT-enabled computing systems.

5.Conclusion

To mitigate the security challenges depicted in multi-cloud environment, this paper proposes an adaptive cyber threats detection framework on a CNN-LSTM hybrid deep learning model. We showcase the advantages of employing deep learning methods in our analysis and highlight their capabilities for advanced intrusion detection that, beyond the classical solutions, bring new features to the table. The proposed model that combines CNN for spatial feature extraction and LSTM for temporal sequence analysis is highly effective in detecting both known and unknown cyber threats with a high degree of accuracy. By adding an adaptive learning mechanism, the model can intelligently evolve according to various attack patterns. Experimental results confirm that the proposed approach surpasses the performance of traditional machine learning approaches, as well as standalone deep learning models with respect to accuracy, false positive rate and response time. Furthermore, the framework exhibits good scalability and steady performance across different cloud platforms suitable for deployment in real-world applications. Broadly, this work lays the groundwork for the creation of smart, autonomous and resilient cyber defense solutions, establishing a solid base for securing contemporary multi-cloud architectures against ever more sophisticated adversaries.

References

[1] Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors* **2023**, *23*, 4117. [**Google Scholar**] [**CrossRef**] [**PubMed**]

[2] Conti, M.; Dargahi, T.; Dehghantanha, A. *Cyber Threat Intelligence: Challenges and Opportunities*; Springer International Publishing: New York, NY, USA, 2018. [**Google Scholar**]

[3] Osama, F.; Dogdu, E. Intrusion detection using big data and deep learning techniques. In *Proceedings of the 2019 ACM Southeast Conference*; AMC: New York, NY, USA, 2019; pp. 86–93. [**Google Scholar**]

[4] Kaur, G.; Lashkari, A.H.; Rahali, A. Intrusion traffic detection and characterization using deep image learning. In Proceedings of the 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 17–22 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 55–62. [**Google Scholar**]

[5] Internet Security Threat Report. Available online: **https://docs.broadcom.com/doc/istr-23-2018-en** (accessed on 18 July 2022).

[6] Attaran, M. The impact of 5G on the evolution of intelligent automation and industry digitization. *J. Ambient Intell. Hum. Comput.* **2023**, *14*, 5977–5993. [**Google Scholar**] [**CrossRef**]

[7] Khan, S.; Silva, P. Internet of Things (IoT) and Its Influence on Digital Transformation. *J. Emerg. Technol. Digit. Transform.* **2023**, *2*, 114–125. [**Google Scholar**]

[8] Gohar, A.; Nencioni, G. The role of 5G technologies in a smart city: The case for intelligent transportation system. *Sustainability* **2021**, *13*, 5188. [**Google Scholar**] [**CrossRef**]

[9] Oladimeji, D.; Gupta, K.; Kose, N.A.; Gundogan, K.; Ge, L.; Liang, F. Smart transportation: An overview of technologies and applications. *Sensors* **2023**, *23*, 3880. [**Google Scholar**] [**CrossRef**] [**PubMed**]

[10] Obafemi, A. Internet of Things (IoT) in Smart Factories: A Systematic Review. *Res. J. Civ. Ind. Mech. Eng.* **2024**, *1*, 09–20. [**Google Scholar**]

[11] Khalil, R.A.; Saeed, N.; Masood, M.; Fard, Y.M.; Alouini, M.S.; Al-Naffouri, T.Y. Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications. *IEEE Internet Things J.* **2021**, *8*, 11016–11040. [**Google Scholar**] [**CrossRef**]

[12] Marcu, O.C.; Bouvry, P. Big Data Stream Processing. Doctoral Dissertation, University of Luxembourg, Luxembourg, 2024. [**Google Scholar**]

[13] Shahraki, A.; Abbasi, M.; Taherkordi, A.; Jurcut, A.D. A comparative study on online machine learning techniques for network traffic streams analysis. *Comput. Netw.* **2022**, *207*, 108836. [**Google Scholar**] [**CrossRef**]

[14] Chukwunweike, J.N.; Adewale, A.A.; Osamuyi, O. Advanced modelling and recurrent analysis in network security: Scrutiny of data and fault resolution. *World J. Adv. Res. Rev.* **2024**, *23*, 2373–2390. [**Google Scholar**] [**CrossRef**]

[15] Miloslavskaya, N. Stream data analytics for network attacks' prediction. *Procedia Comput. Sci.* **2020**, *169*, 57–62. [**Google Scholar**] [**CrossRef**]

[16] Vanickis, R.; Jacob, P.; Dehghanzadeh, S.; Lee, B. Access control policy enforcement for zero-trust-networking. In Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, 21–22 June 2018. [**Google Scholar**]

[17] Li, S.; Iqbal, M.; Saxena, N. Future industry internet of things with zero-trust security. *Inf. Syst. Front.* **2022**, *26*, 1653–1666. [**Google Scholar**] [**CrossRef**]

[18] L, G.; White, K. Detection of ransomware using machine learning techniques. *J. Comput. Secur.* **2022**, *30*, 189–201. [**Google Scholar**]

[19] Abdulsalam, Y.S.; Hedabou, M. Security and privacy in cloud computing: Technical review. *Future Internet* **2022**, *14*, 11. [**Google Scholar**] [**CrossRef**]