

# International Journal of Information Technology, Research and Applications (IJITRA)

**Zafar Iqbal, Ahtasham Sajid, Muhammad Nauman Zakki, Adeel Zafar, Arshad Mehmood, (2024). Role of Machine and Deep Learning Algorithms in Secure Intrusion Detection Systems (IDS) for IOT & Smart Cities, 3(4), 01-16.**

**ISSN: 2583 5343**

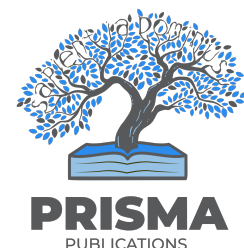
**DOI: 10.59461/ijitra.v3i4.111**

The online version of this article can be found at:  
<https://www.ijitra.com/index.php/ijitra/issue/archive>

Published by:  
PRISMA Publications

IJITRA is an Open Access publication. It may be read, copied, and distributed free of charge according to the conditions of the Creative Commons Attribution 4.0 International license.

**International Journal of Information Technology, Research and Applications (IJITRA)** is a journal that publishes articles which contribute new theoretical results in all the areas of Computer Science, Communication Network and Information Technology. Research paper and articles on Big Data, Machine Learning, IOT, Blockchain, Network Security, Optical Integrated Circuits, and Artificial Intelligence are in prime position.



<https://www.prismapublications.com/>

**Journal homepage:** <https://ijitra.com>

# Role of Machine and Deep Learning Algorithms in Secure Intrusion Detection Systems (IDS) for IOT & Smart Cities

Zafar Iqbal<sup>1</sup>, Ahthasham Sajid<sup>1</sup>, Muhammad Nauman Zakki<sup>1</sup>, Adeel Zafar<sup>2</sup>, Arshad Mehmood<sup>1</sup>

<sup>1</sup> Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

<sup>2</sup> Department of Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

## Article Info

### Article history:

Received September 26, 2024

Revised October 15, 2024

Accepted October 20, 2024

### Keywords:

Machine Learning  
Intrusion Detection Systems,  
IoT Security,  
Smart Cities,  
Smart Farming

## ABSTRACT

In this study the authors have examines various machine learning algorithms that could be used in IDS for making secure IoT and Smart Cities. The study examines various deep learning architectures of supervised, unsupervised, and semi-supervised learning methods to improve security and resource usage. Federated learning, edge computing, explainable AI, adversarial machine learning defense, and transfer learning are also explored for smart farming and IoT challenges. Machine learning has the potential to improve security and agricultural sustainability, but it must be researched and developed. The objective of this research is to explore and analyze the effectiveness of machine learning algorithms in enhancing Intrusion Detection Systems (IDS) for securing IoT environments and smart cities.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Dr. Ahthasham Sajid

Department of Cyber Security Riphah Institute of System Engineering  
Riphah International University, Islamabad, Pakistan

Email: ahthasham.sajid@riphah.edu.pk

## 1. INTRODUCTION

A new urban planning paradigm aims to create "smart cities" that leverage cutting-edge ICT to enhance city inhabitants' lives. IoT, which permits real-time data collecting, sharing, and analysis via networked systems and devices, is crucial to this transition [1]. IDC estimates a global smart city investment of \$158 billion by 2022 [2]. Internet-connected smart cities improve resource management, public services, and city life. According to research, various cities worldwide are benefiting from Internet of Things applications in energy distribution, rubbish disposal, and traffic management [3].

Smart cities rely heavily on networked systems and IoT devices, making network security crucial. The enormous quantity and variety of linked devices increases the cyberattack surface. Gartner predicts that by 2025, there will be 75 billion linked devices, necessitating more advanced security [4]. Smart cities need network security to safeguard sensitive data, service availability and integrity, and citizens' privacy. Insufficient security can cause data breaches, service outages, and financial losses [5]. The 2016 Mirai botnet attack leveraged Internet of Things devices to exploit network security weaknesses and disrupt networks [6]. Protecting smart city networks requires intrusion detection systems (IDS). Intrusion detection systems (IDS) monitor unusual or harmful activity to defend networks from cyberattacks. Intrusion detection systems (IDS) include two main types: anomaly-based detection, which looks for unusual events, and signature-based detection, which matches incoming data to known hostile behaviour patterns [7]. Further research states that signature-based intrusion detection systems are good at recognizing existing hazards, whereas anomaly-based systems are better at finding new threats [7].

Some smart city authors have emphasized intrusion detection systems. According to a research study, intrusion detection systems (IDS) are crucial cybersecurity solutions for urban IoT network safety and functioning [8]. Another research emphasizes the relevance of intrusion detection systems (IDS) in preventing invasions by alerting users to potential dangers and offering remedies [9]. These systems are necessary to preserve smart city infrastructures' integrity and reliability. Figure 1 shows a simple IDS system working.

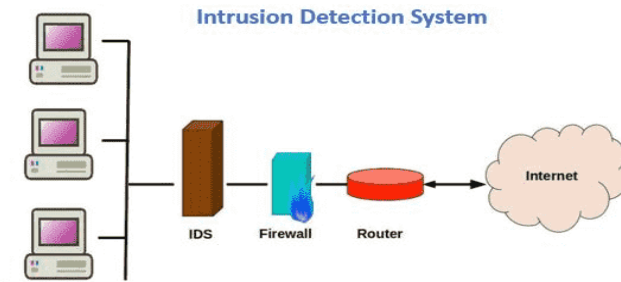


Figure 1: Working of Intrusion Detection System [9]

### Research Contribution:

- Review on machine learning algorithms for intrusion detection systems (IDS) targeting IoT and smart city security. Section 2, describe how machine learning algorithms enhance IDS threat detection in smart cities by reviewing several research.
- Examine critically the existing key studies. Section 3, critically assess significant research' techniques and conclusions on IDS efficacy in smart cities.
- Discuss strategies to enhance IDS. The literature study in Section 3 discuss existing IDS difficulties and possible solutions, notably using machine learning.
- Contribute to ongoing discussions on protecting smart city networks. It is added to the discussion on smart city security in the face of growing cyber threats by synthesising the examined material.
- Ensure efficient and safe operation of smart city networks despite evolving cyber threats. Section 4 will emphasise the need of strong IDS and provide practical ideas for future research and practice to keep smart city networks secure and functioning.

The rest of the sections of this article are as follows: Section 2 presents relevant literature findings from the field. Section 3 reviews the literature to solve objectives. Section 4 concludes the article with a summary of key points and suggestions.

## 2. RELATED WORK

This section discusses the work done in the field of machine learning-based Intrusion Detection Systems (IDS) for IoT and smart city security.

Research [10] categorized intrusion detection system (IDS) machine learning approaches as supervised, unsupervised, and hybrid. As they noted, supervised learning methods like Decision Trees and Support Vector Machines (SVM) are best at recognizing patterns of earlier attacks but less so at detecting new ones. The study showed that unsupervised learning can detect zero-day risks, but it also had significant false positive rates. This study provides a basic overview of existing techniques, but it does not evaluate particular algorithms in IoT scenarios.

Focusing on CNNs and RNNs, another research examined how IDS may benefit from deep learning [11]. Deep learning models outperformed machine learning methods in detection accuracy and data management. Although deep learning models have various IoT applications, the study found that training

them demands many computer resources. The complex approaches it investigates make this study valuable even if it does not address deployment concerns.

A study [12] examined IoT IDS using machine learning for anomaly detection. PCA and k-means clustering were used to find unusual activities. The study showed that these methods might detect unusual tendencies that may imply an attack. The high rate of false positives might generate alarm fatigue. Although restricted, this study's focus on unsupervised techniques is a strength since they reveal new hazards. Another study [13] examined Random Forests, Naive Bayes, and Support Vector Machines for intrusion detection systems. These methods were evaluated for computational efficiency, false positive rate, and detection accuracy. The study indicated that Random Forests balanced performance and accuracy well. The study's comparison results are beneficial, but deep learning and its potential in modern IDS applications remain understudied.

Research also [14] examined how machine learning might enhance IoT security. A combined strategy of supervised and unsupervised learning increased detection rates. Hybrid techniques reduced false positives and improved threat identification for existing and emerging threats. This study shows that combining approaches may be useful, but additional testing in other IoT situations might improve it. Another researcher [15] developed a neural network-based intrusion detection system (IDS) to regulate metropolitan IoT device traffic patterns. Although expanding the approach to larger networks was challenging, their neural network model detected intrusions with high accuracy. Scalability is still an issue, but this research's focus on smart cities is its strength.

A study [16] released a semi-supervised learning-based adaptive IDS for IoT. Their system adapts to diverse attacks by learning from new data. This strategy progressively boosted detection rates while reducing false positives. Its approach adapts nicely to IoT situations, one of its strengths. However, data collection and model updates may be resource-intensive. Research also [17] examined how IoT IDS uses ensemble learning. Adding more classifiers boosted detection rates and made it more robust to attacks. Ensemble techniques may increase system robustness and false positives, according to studies. This technique has promise, but it requires many training data and is computationally expensive. Research [18] identified IoT network abnormalities using Autoencoders and other deep-learning methods. Their solution effectively discovered outliers, demonstrating deep learning's potential in complex IoT data management. According to the study, deep learning models demand many computer resources to train and deploy; thus, they may not be suitable for all Internet of Things devices.

Another study [19] recommended lightweight intrusion detection methods for low-resource IoT devices. A simple neural network model was presented to balance detection accuracy and resource utilization. The study focused on preserving security without exhausting device resources and showed promising results. Despite having lower detection accuracy than more sophisticated models, this research is useful since it realistically manages resource constraints. A study [20] developed a deep learning-based IDS for smart cities. They employed a deep belief network to find traffic outliers. The technology was accurate and adaptable to diverse network traffic. The study revealed some possible benefits, but it also noted that it needed a lot of training data and computing resources, which may limit its utility. This study's focus on smart city settings provides useful insights into urban network security.

Another researcher [21] examined different machine-learning approaches for IoT intrusion detection systems (IDS). In numerous research, they discussed the pros and cons of SVMs, DTs, and k-means clustering. Since no algorithm did well across the board, the study shows the need for context-specific algorithms. This research provides useful comparative insights, but it also suggests that hybrid methods may provide the best long-term outcomes. One author [22] used machine learning and stream processing to detect intrusions in real-time. Their technique enabled quick intrusion detection and response, securing IoT networks. Despite its success, the research showed the challenges of real-time processing of enormous data volumes. Real-time capabilities are a major benefit of this technique, although scalability remains a challenge.

Machine learning for Internet of things intrusion detection systems was proposed by another researcher [23]. Integrating many detection methods within its design provides complete intrusion detection. The study found higher detection rates and fewer false positives, which is promising. Its broad approach makes the research strong, even if it does not address actual implementation concerns. Research [24] examined smart home IDS using support vector machines and k-means clustering. By considering smart home device traffic patterns, they created a system that correctly recognized intruders. Research shows that machine learning may enhance home IoT network security. Its focus on an IoT application makes this research strong, even if it does not examine transferability. Table 1 shows a few more important past studies critically:

**Table 1:** Critical Analysis of Literature

Year	Ref.	Aim of Paper & Key Methods	Key Results	Limitations
2024	[26]	Investigate the application of edge computing in IoT IDS using edge computing and ML.	Utilized edge computing to enhance real-time IDS performance in IoT Reduced data transmission and processing latency	Limited scalability due to edge device constraints
2024	[27]	Study the use of blockchain technology for IoT IDS using blockchain and distributed ledger.	Utilized blockchain for secure and tamper-resistant logging in IoT IDS Enhanced data integrity and immutability	Increased computational overhead due to blockchain operations
2024	[28]	Investigate the role of reinforcement learning in IoT IDS using reinforcement learning.	Utilized reinforcement learning for adaptive and self-learning IDS in IoT Improved detection accuracy over time through learning from feedback	Requires significant computational resources for learning and adaptation
2024	[29]	Explore the use of anomaly-based techniques for IoT IDS using anomaly detection methods.	Leveraged anomaly-based techniques for detecting unusual behaviors in IoT networks Effectively identified previously unseen threats.	higher false positive rates compared to signature-based approaches
2020	[25]	A lightweight IDS for IoT devices using feature extraction and machine learning	Lightweight IDS suitable for resource constrained IoT devices Achieved high detection accuracy with minimal resource consumption	sacrifices detection accuracy for resource optimization

### 2.1 Research Gap

The past research lack in various aspects. First and foremost, smart cities need scalable intrusion detection systems to handle huge volumes of heterogeneous data from IoT devices. It is also studied neural networks for smart city applications; however, they did not address scalability in larger networks and different situations. As, deep learning models' high computational requirements make resource-constrained IoT devices struggle. Second, large false positive rates are a key challenge for anomaly-based detection systems. Also review discovered this constraint, which may create alarm fatigue and reduce IDS efficiency. False positives must be reduced while detection rates remain high. Thirdly, most present research lacks real-world support. Research employs theoretical and simulated settings to give insights, but they cannot fully reflect real-world IoT networks. Practical deployment issues like learning and adapting need more study. This review paper examines machine learning approaches in IoT intrusion detection systems (IDS) and smart city network security to solve these gaps. This research combines and analyzes prior studies to find excellent methods and ways to improve them.

### 3. REVIEW OF MACHINE LEARNING ALGORITHMS IN IDS FOR IOT AND SMART CITIES

This section provides various studies to form a review of Machine Learning Algorithms utilized in IDS for IoT and Smart Cities.

Figure 2 shows the structure of this Rivev performed.

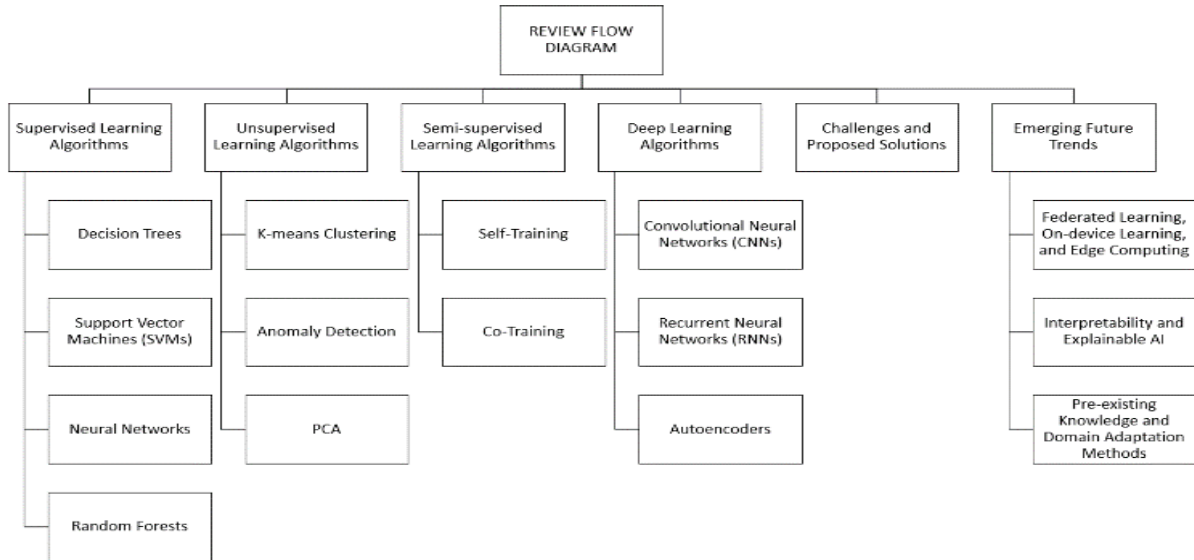
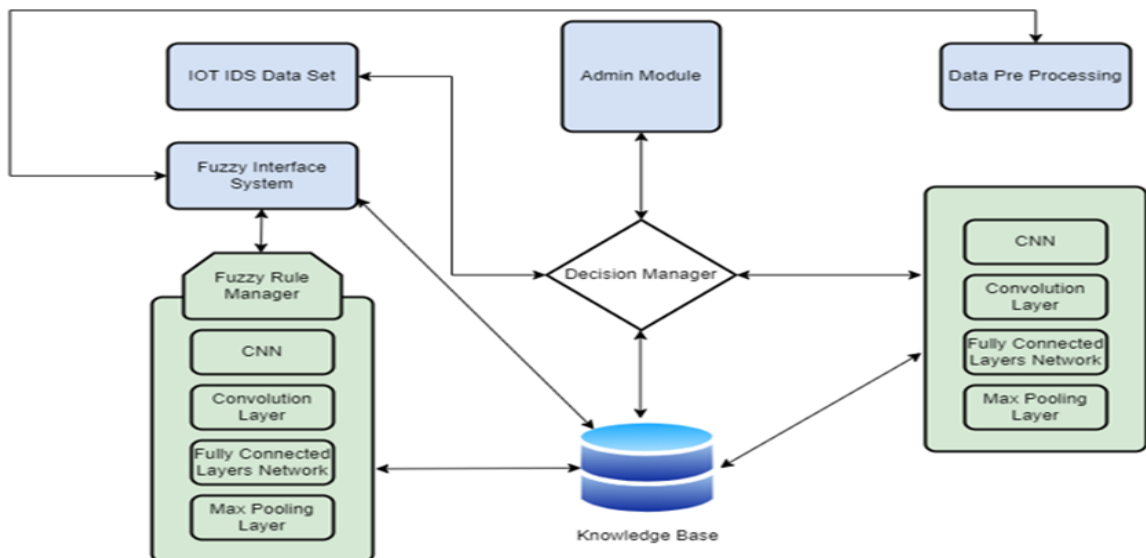


Figure 2: Process Flow Diagram

#### 3.1 Supervised Learning Algorithms

There are several methods of supervised learning algorithms as performed and discussed by various researchers. Decision Trees, a staple of intrusion detection system (IDS) investigations, secure the IoT and smart cities. Decision Trees are supervised learning methods that recognize attack patterns [30]. The strategy is simple to comprehend and evaluate, giving security analysts insight into IDS decision-making. A comparative research [31] found decision trees beneficial in intrusion detection. Overfitting may lead Decision Trees to function differently in different circumstances, according to the research.

Support Vector Machines (SVMs) are famous for data classification. Another research [32] evaluated SVMs in intrusion detection systems and noted their computational efficiency and accuracy. The



advantage of SVMs is their capacity to create optimal decision boundaries, which increase generalization. A study [33] investigated SVMs for Internet of Things security to detect risks and reduce false positives. However, kernel settings may affect SVM performance, so tweak them carefully.

### Figure 3: Architecture Design

Neural networks are now a powerful intrusion detection [34] method due to their pattern-spotting abilities. Research p tested a neural network-based IDS. When tuned to urban IoT device traffic patterns, it detected intrusions more accurately. Due to their variety and flexibility, neural networks can identify small dangers. However, another study [35] highlighted that neural networks are resource-intensive, highlighting data and processing issues. Despite this drawback, neural networks may increase Smart City and IoT IDS performance.

Random Forests are useful for intrusion detection investigations because of their ensemble learning. In their ensemble learning research, Research [36] showed how Random Forests may increase detection and system resilience. This method may improve generality and reduce overfitting over particular decision trees. In training and inference, Random Forests provide a significant computational challenge. Another research [37] presents lightweight intrusion detection methods based on Random Forests' high accuracy-to-resource consumption ratio. Random Forests is a great intrusion detection system (IDS) for IoT and smart city security despite its drawbacks.

### 3.2 Unsupervised Learning Algorithms

Machine learning uses unsupervised learning algorithms to find patterns in unlabeled data without human interaction. Unsupervised learning finds insights, correlations, and outliers using raw, unstructured data, whereas supervised learning trains algorithms using labelled samples. As academics have noted, it includes many methods.

K-means clustering aggregates data by similarity to reveal dataset grouping trends. It is basic unsupervised learning. Research [38] showed how IoT intrusion detection systems (IDS) using K-means clustering can identify unusual activity that may indicate an assault. It shows that the algorithm can detect suspicious IoT network activities. Clustering is hampered by high-dimensional data and identifying the optimal K clusters.

Researchers also study how Smart Cities may utilize K-means clustering to find network abnormalities [39]. Their primary point was how successfully the system detected questionable network activities and enabled proactive protection. Despite its strengths, K-means clustering may not detect complex and dynamic threats; hence, other methodologies are required for intrusion detection.

Researchers also examined K-means clustering for industrial IoT anomaly detection [40]. Their research revealed that the system might identify unexpected industrial actions to increase operational security. However, academics are still working to make K-means clustering work in the complex and ever-changing IoT ecosystem.

Another method is Anomaly detection technologies are essential for detecting new threats and zero-day attacks. Research showed real-time IoT intrusion detection using machine learning and stream processing [41]. Their research shows that anomaly detection quickly detects and reduces security vulnerabilities. Due to high false positive rates, anomaly detection algorithms must be improved to save operating costs.

Another study [42] reviewed an all-encompassing intrusion detection system that employs many anomaly detection methods to defend the Internet of Things. Their study showed that combining detection methods improved threat detection rates and reduced false positives. Anomaly detection technologies function well, but scalability is a concern for big IoT setups.

A study also [44] examined anomaly detection in car IoT settings for traffic monitoring and security. By detecting suspicious behaviour, anomaly detection enhanced road safety and network resilience. Identifying legitimate irregularities from malicious attacks is tough in real-world deployment circumstances.

PCA is a fundamental dimensionality reduction method that extracts essential properties from high-dimensional data. Author [45] introduced a lightweight IDS for IoT devices that use PCA for feature extraction to reduce computational overhead. The system architecture is shown in Figure 3. They found that principal component analysis (PCA) simplifies data processing in intrusion detection systems. In complex networks, PCA may experience data loss and decreased discrimination.



Another researcher [46] examined smart city network anomalies using PCA. The algorithm's capacity to extract key properties from enormous network data speeds up threat detection and response. Finding the balance between dimensionality reduction and information retention and understanding principal component analysis (PCA) feature interpretability needs further investigation.

A study also examined how PCA may detect patient monitoring system abnormalities in healthcare IoT contexts [47]. Their study showed that principal component analysis (PCA) may detect unusual physiological patterns, which may help diagnose health issues early. Finding the right balance between computer efficiency and detection accuracy is crucial in real-time healthcare applications.

### 3.3 Semi-supervised Learning Algorithms

Semi-supervised learning algorithms provide a new paradigm by combining supervised and unsupervised learning. Semi-supervised learning combines both supervised and unsupervised algorithms to predict [48]. These algorithms excel when unlabeled data is abundant, but labelled data is scarce or expensive. Using labelled and unlabeled data, semi-supervised learning techniques train models more cheaply and efficiently than supervised methods.

Self-training, a semi-supervised learning strategy, lets a model accurately categorize unlabeled data points to contribute to its training set after initial training on a small labelled dataset. Researchers [48] introduced a semi-supervised learning-based adaptive IDS for the Internet of Things (IoT) by showing how self-training may steadily boost detection rates and decrease false positives. Figure 4 shows the flow diagram of the research. Self-training algorithms must carefully pick confidence predictions and avoid error propagation.

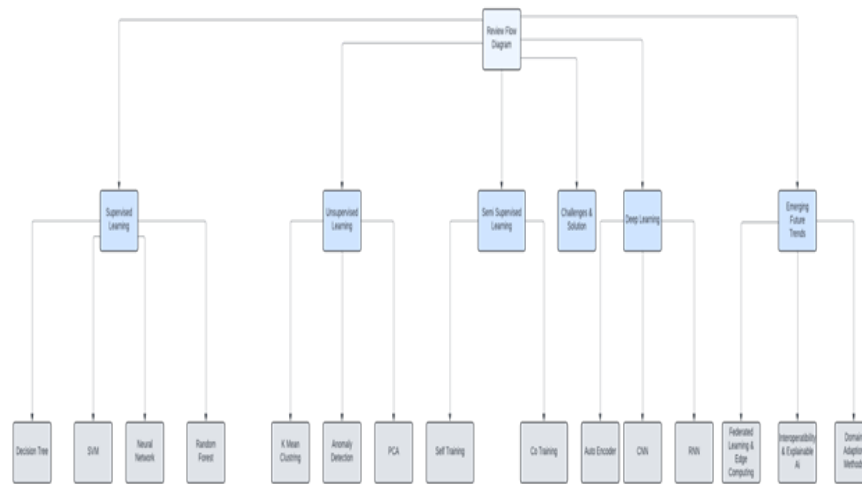


Figure 4: Process Flow Diagram

Another study [49] examined how Smart City self-training improves traffic flow anomaly identification. Class imbalance and uncertainty estimation must be addressed for its implementation to succeed despite its numerous advantages. The author utilized self-training to healthcare data for sickness diagnosis to illustrate how unlabeled patient information might increase diagnostic accuracy [49]. Model resilience and self-labelled example trustworthiness in ever-changing healthcare environments are currently being studied [49].

Co-training uses several data viewpoints to train classifiers repeatedly in semi-supervised learning. Labeled examples are shared across views to improve model performance. Through co-training in the Internet of Things security, research [50] demonstrated that supervised and unsupervised learning may improve detection rates. Their study highlighted the benefits of co-training in complementary data sources. However, classifier diversity and viewpoint selection must be addressed.

Research [51] also performed network intrusion detection in Smart Cities, showing how co-training with many data modalities improves detection accuracy. Despite its value, view dependency and limited unlabeled data availability must be addressed for widespread adoption. The author also investigated co-training in industrial IoT contexts for production process fault identification, showing that the diversity of



sensor data may increase predictive maintenance abilities [52]. Scalability and model interpretability in large-scale industrial environments need further study.

### 3.4 Deep Learning Algorithms

Deep learning algorithms, which mimic the human brain, have transformed computer vision, pattern recognition, and natural language processing. Deep learning can extract precise patterns and features from complex datasets to enhance intrusion detection systems (IDS) in cybersecurity.

Convolutional neural networks (CNNs) deep neural networks are good in image classification, object identification, and anomaly detection. In intrusion detection systems, research [53] found CNNs better at detecting cyberattacks and network anomalies. They showed that convolutional neural networks (CNNs) may automatically learn discriminative features from unprocessed network traffic data to increase detection accuracy and reduce the requirement for feature engineers [53]. Computational complexity and the necessity for large, labelled datasets may restrict CNN-based intrusion detection system scalability in resource-constrained environments.

Just like that, another research [54] proposed a deep learning-based smart city identification system. Convolutional neural networks (CNNs) analyze network traffic to detect suspicious activities. CNNs may identify breaches and enhance urban network security, they found. Despite promising results, convolutional neural network (CNN)-based intrusion detection systems still suffer adversarial attacks and model interpretability issues.

By researching IoT anomaly detection using convolutional neural networks (CNNs), researchers [55] showed how CNNs can automatically extract meaningful characteristics from sensor data streams. They showed that CNNs can detect slight deviations from the norm, which might help identify and reduce hazards. Concept drift and data heterogeneity may affect the long-term dependability of convolutional neural network (CNN) anomaly detection systems.

Recurrent Neural Networks (RNNs) employ feedback loops to evaluate sequential input and record contextual and temporal relationships. Researcher [56] constructed an RNN-based intrusion detection system to manage metropolitan IoT device traffic to show their usefulness in smart city settings. Figure 5 shows a conceptual map of the study. Their research showed that RNNs can reflect complex temporal correlations in network traffic data by enhancing intrusion detection accuracy. However, long training times and fading gradients may render RNN-based IDS ineffective in practice.

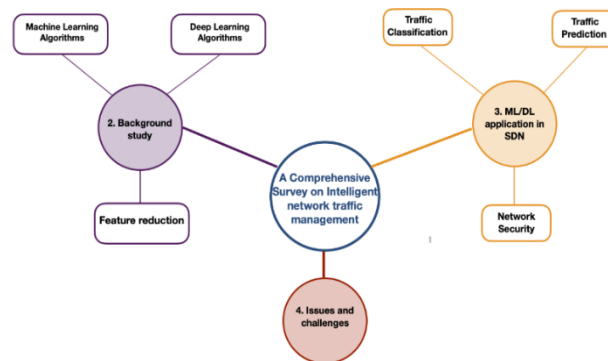


Figure 5: Conceptual map [56]

Another research [57] showed how recurrent models may improve threat detection by collecting sequential patterns in network data in their research on RNNs and IoT security. Their study highlighted RNNs' time-series data handling and cyber risk detection capabilities. The generalization performance of RNN-based intrusion detection systems may be affected by model overfitting and data sparsity.

Autoencoders are unsupervised learning algorithms that encode input data into a lower-dimensional latent space and reconstruct it to develop efficient representations. On such study [58] showed how autoencoders can capture data distributions and uncover strange anomaly detection patterns for IoT intrusion detection systems. Their results showed that autoencoders may detect new cyber dangers and reduce false positives. Hyperparameter tinkering and model interpretability may hinder autoencoder-based IDS uptake.

Researchers [59] provide a review of an autoencoder-based anomaly detection system for Smart Cities using unsupervised learning. This framework detects network irregularities and security vulnerabilities. Their study showed that autoencoders can learn compact representations of network traffic data to improve urban anomaly detection. However, further study is required to address concerns regarding autoencoder-based intrusion detection systems' susceptibility to malicious attacks and data disruptions.

Another study [60] showed how autoencoders could detect tiny changes in IoT network behaviour in real-time for intrusion detection. Their work highlighted the benefits of unsupervised learning for IoT security against emerging cyber threats. Autoencoder-based IDS may not work for large-scale IoT deployments owing to computational expense and model scalability.

### 3.5 Implementing Challenges and likely Solutions

Table 2 critically reviews and summarizes the challenges posed by Machine learning algorithms in IDS for IoT and Smart Cities as discussed by various authors [61-66], along with the restrictions those challenges pose and solutions as described by authors [67-69] for machine learning-based intrusion detection systems (IDS) for the Internet of Things (IoT) and smart cities. Each difficulty level and machine learning method restrictions are accurately characterized. Additionally, the recommended solutions are expanded to provide information on how to overcome these limits and maximize intrusion detection system deployment in Smart City and Internet of Things contexts.

**Table 2:** Challenges and Existing Solutions

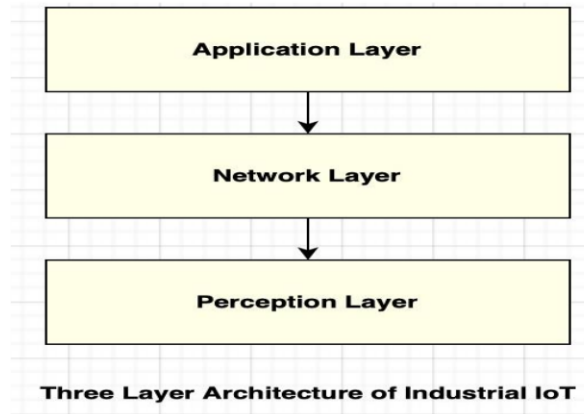
Challenge Name	Machine Learning Algorithms	Limitations Identified	Likely Solutions
Technical challenges in deploying machine learning-based IDS in IoT [61-62]	Decision Trees	Overfitting may lead to inconsistent performance across different contexts.	Regularization techniques (e.g., pruning) can mitigate overfitting and enhance generalization [67].
	Support Vector Machines (SVMs)	Performance may be sensitive to kernel settings.	Parameter optimization methods can fine-tune kernel settings for improved performance [67].
	Neural Networks	Resource-intensive nature may pose challenges in processing and scalability.	Distributed computing frameworks and optimization of neural network architectures can alleviate computational burdens and enhance scalability [67].
	Random Forests	Computational complexity may limit scalability, particularly in large-scale deployments.	Optimization of ensemble learning techniques and parallel processing can enhance scalability and efficiency [68].
	K-means Clustering	Challenges with high-dimensional data and selection of optimal cluster number.	Advanced clustering algorithms and dimensionality reduction techniques can address these challenges [68].
	Anomaly Detection	High false positive rates may increase operational costs and impact system efficiency.	Refinement of anomaly detection algorithms and adaptive thresholding can mitigate false positives and improve detection accuracy [68].
	PCA (Principal Component Analysis)	Reduced discrimination and data loss in complex networks.	Advanced PCA variants and feature engineering methods can improve discrimination and preserve information [68].

Security and privacy concerns [63-64]	Self-training	Error propagation and model reliability issues in dynamic environments.	Robust confidence estimation mechanisms and continuous model retraining can enhance model reliability and adaptability [69].
	Co-training	Dependence on data diversity and limited availability of unlabeled data.	Active learning strategies and data augmentation techniques can enrich labelled data and improve model performance [69].
	Autoencoders	Vulnerability to adversarial attacks, hyperparameter tuning challenges, and model interpretability issues.	Adversarial training, interpretability enhancements, and robustness validation techniques can address these concerns [69].
Scalability challenges [65-66]	Deep Learning Algorithms (e.g., CNNs, RNNs)	Increased computational and memory requirements hinder scalability in resource-constrained environments.	Optimization of model architectures, parameter tuning, and utilization of distributed computing frameworks can enhance scalability [69].
	Ensemble Learning (e.g., Random Forests)	Complexity in integrating multiple models and managing ensemble diversity affects scalability and deployment.	Streamlining ensemble methods, model selection strategies, and efficient parameter tuning can improve scalability and efficiency [69].
	Real-time Processing	Processing time constraints and latency issues may impact the real-time effectiveness of IDS in dynamic environments.	Implementing optimized algorithms, hardware acceleration, and parallel processing can enhance real-time performance [69].

### 3.6 Emerging Future Trends in Machine Learning in IDS for IoT and Smart Farming

Machine learning can make the Internet of Things (IoT) more secure and smart farming more advanced. Various researchers show that these trends will enhance agricultural firms' resource utilization and decision-making while reducing new risks.

Federated learning transforms collaborative model training across distributed IoT devices and agricultural sensors. Federated learning examined [70] shows how devices may learn from local data while maintaining user privacy and enhancing IoT security. The three-tier architecture of which is shown in Figure 6. This technology allows smart farming's agricultural sensors to "learn" from one other and adapt to their environment, enabling more informed, tailored field peripheral choices.



**Figure 6:** Three-tier architecture [70]

Smart farming and IoT security applications may benefit from on-device learning and edge computing for real-time responsiveness and low latency. Another study [71] examines the benefits of applying modest machine-learning models to IoT devices and agricultural sensors. Edge computing allows localized data processing and analysis, allowing IoT devices to detect security threats and irregularities automatically. It permits timely, context-aware agricultural actions.

Interpretability and explainable AI (XAI) may make machine learning models more visible and understandable, encouraging collaboration and confidence in smart farming and IoT security. Researchers [72-73] show how security analysts and farmers need XAI to comprehend model decisions. Interpretable machine learning models let stakeholders find and solve IoT security risks rapidly. Transparent AI technologies help farmers make wise agricultural choices by providing crop health, soil, and environmental data.

Securing IoT and Smart Farming from Advanced Cyberattacks Needs Strong Adversarial Machine Learning Defenses. One such study [74] innovative defensive approaches, focusing on robust model training and adversarial example identification. Adversarial defensive methods assist intrusion detection systems in resisting manipulation and evasion, keeping IoT networks safe. These protections prevent agricultural systems from harmful attacks that threaten data integrity or decision-making, keeping smart farming technology trustworthy and successful.

Using Pre-Existing Knowledge and Domain Adaptation: These two methodologies are essential for adapting machine learning models to IoT and agriculture. Research [75] transfers learning's capacity to generalize models and transfer knowledge from related fields for IoT security. Smart farming uses domain adaptation techniques to incorporate diverse data sources and environmental factors smoothly, making machine learning models more resilient and adaptable to a variety of farming situations and making knowledge transfer easier.

#### 4. CONCLUSION

In conclusion, this review paper explores machine learning methods in IDS for the IoT and Smart Cities. It illuminates current research, challenges, and future directions. A thorough literature study found that machine learning can improve IoT smart farming and security. Researchers have used supervised, unsupervised, and semi-supervised learning approaches to recognize intrusions and irregularities, each having pros and cons. Transfer learning, adversarial machine learning defence, explainable AI, federated learning, edge computing, and deep learning architectures may help smart farming and IoT applications maximize resource consumption and manage growing dangers. Additional research is needed to solve data privacy, model interpretability, and scalability challenges. The paper suggests that interdisciplinary collaboration and innovation are essential for smart city IoT ecosystem security and agricultural sustainability.

## 5. ACKNOWLEDGMENTS

Me **Mr. Zafar Iqbal** as an author of this review paper acknowledge numerous devoted researchers and academic institutions for their contributions to machine learning, IoT security, and smart farming. I am forever thankful to Assistant Professor **Dr. Ahtasham Sajid** for his kind guidance, support and motivation to accomplish this research write-up as good quality work.

### References

- [1]. Bauer, M., Sanchez, L., and Song, J., 2021. IoT-Enabled Smart Cities: Evolution and Outlook. *Sensors*, 21(13), p.4511. Available at: <https://doi.org/10.3390/s21134511>.
- [2]. IDC Forecasts Smart Cities Spending to Reach \$158 Billion in 2022, with Singapore, Tokyo, and New York City Among Top Spenders, 2024. *Business Wire*. Available at: <https://www.businesswire.com/news/home/20180723005083/en/IDC-Forecasts-Smart-Cities-Spending-to-Reach-158-Billion-in-2022-with-Singapore-Tokyo-and-New-York-City-Among-Top-Spenders> [Accessed 3 Jun. 2024].
- [3]. Mishra, P. and Singh, G., 2023. Energy Management Systems in Sustainable Smart Cities Based on the Internet of Energy: A Technical Review. *Energies*, 16(19), p.6903. Available at: <https://doi.org/10.3390/en16196903>.
- [4]. Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A., and Brown, J., 2020. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers*, 9(2), p.44. Available at: <https://doi.org/10.3390/computers9020044>.
- [5]. Ismagilova, E., Hughes, L., Rana, N.P., and Dwivedi, Y.K., 2020. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers*, 24, Available at: <https://doi.org/10.1007/s10796-020-10044-1>.
- [6]. D21DCS151, 2023. A case study on Mirai Botnet Attack of 2016. *Medium*. Available at: <https://medium.com/@d21dcs151/a-case-study-on-mirai-botnet-attack-of-2016-4b66630e6508> [Accessed 10 Apr. 2023].
- [7]. Heidari, A. and Jamali, M.A.J., 2022. Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*. Available at: <https://doi.org/10.1007/s10586-022-03776-z>.
- [8]. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., and Wahab, A., 2020. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics*, 9(7), p.1177. Available at: <https://doi.org/10.3390/electronics9071177>.
- [9]. Chang, V. et al., 2022. A Survey on Intrusion Detection Systems for Fog and Cloud Computing. *Future Internet*, 14(3), p.89. Available at: <https://doi.org/10.3390/fi14030089>.
- [10]. Abdullah, D.M. and Abdulazeez, A.M., 2021. Machine Learning Applications based on SVM Classification: A Review. *Qubahan Academic Journal*, 1(2), pp.81–90. Available at: <https://doi.org/10.48161/qaj.v1n2a50>.
- [11]. Ahmad, Z., Khan, A.S., Shiang, C.W., Abdullah, J., and Ahmad, F., 2020. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1). Available at: <https://doi.org/10.1002/ett.4150>.
- [12]. Alsoufi, M.A. et al., 2021. Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. *Applied Sciences*, 11(18), p.8383. Available at: <https://doi.org/10.3390/app11188383>.
- [13]. Saranya, T., Sridevi, S., Deisy, C., Chung, T.D., and Khan, M.K.A.A., 2020. Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. *Procedia Computer Science*, 171, pp.1251–1260. Available at: <https://doi.org/10.1016/j.procs.2020.04.133>.
- [14]. Ahmad, R. and Alsmadi, I., 2021. Machine Learning Approaches to IoT Security: A Systematic Literature Review. *Internet of Things*, 14, p.100365. Available at: <https://doi.org/10.1016/j.iot.2021.100365>.
- [15]. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., and Wahab, A., 2020. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics*, 9(7), p.1177. Available at: <https://doi.org/10.3390/electronics9071177>.
- [16]. Mvula, P.K., Branco, P., Jourdan, G.-V., and Viktor, H.L., 2024. A Survey on the Applications of Semi-Supervised Learning to Cyber-Security. *ACM Computing Surveys*. Available at: <https://doi.org/10.1145/3657647>.
- [17]. Tama, B.A. and Lim, S., 2021. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. *Computer Science Review*, 39, p.100357. Available at: <https://doi.org/10.1016/j.cosrev.2020.100357>.
- [18]. Gyamfi, E. and Jurcut, A., 2022. Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. *Sensors*, 22(10), p.3744. Available at: <https://doi.org/10.3390/s22103744>.
- [19]. Malik, R., Singh, Y., Sheikh, Z.A., Anand, P., Singh, P.K., and Workneh, T.C., 2022. An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems. *Journal of Advanced Transportation*, 2022, p.e7892130. Available at: <https://doi.org/10.1155/2022/7892130>.






- [20]. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., and Wahab, A. (2020) 'A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions', *Electronics*, 9(7), p. 1177. doi: [10.3390/electronics9071177](https://doi.org/10.3390/electronics9071177).
- [21]. Santhosh Kumar, S.V.N., Selvi, M., and Kannan, A. (2023) 'A comprehensive survey on machine learning-based intrusion detection systems for secure communication in Internet of Things', *Computational Intelligence and Neuroscience*, 2023, pp. 1–24. <https://doi.org/10.1155/2023/8981988>.
- [22]. Nassiri Abrishamchi, M.A., Zainal, A., Ghaleb, F.A., Qasem, S.N., and Albarrak, A.M. (2022) 'Smart home privacy protection methods against a passive wireless snooping side-channel attack', *Sensors*, 22(21), p. 8564. <https://doi.org/10.3390/s22218564>.
- [23]. Thakkar, A. and Lohiya, R. (2020) 'A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges', *Archives of Computational Methods in Engineering*. <https://doi.org/10.1007/s11831-020-09496-0>.
- [24]. Adeniyi, O., Safaa Sadiq, A., Pillai, P., Aljaidi, M., and Kaiwartya, O. (2024) 'Securing mobile edge computing using hybrid deep learning method', *Computers*, 13(1), pp. 25–25. <https://doi.org/10.3390/computers13010025>.
- [25]. Ahakonye, L.A.C., Nwakanma, C.I., and Kim, D.-S. (2024) 'Tides of blockchain in IoT cybersecurity', *Sensors*, 24(10), p. 3111. <https://doi.org/10.3390/s24103111>.
- [26]. Saadouni, R., Gherbi, C., Aliouat, Z., Harbi, Y., and Khacha, A. (2024) 'Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: A systematic review of the literature', *Cluster Computing*. <https://doi.org/10.1007/s10586-024-04388-5>.
- [27]. Rafique, S.H., Abdallah, A., Musa, N.S., and Murugan, T. (2024) 'Machine learning and deep learning techniques for Internet of Things network anomaly detection—Current research trends', *Sensors*, 24(6), p. 1968. <https://doi.org/10.3390/s24061968>.
- [28]. Chatziamanetoglou, D. and Rantos, K. (2024) 'Cyber threat intelligence on blockchain: A systematic literature review', *Computers*, 13(3), p. 60. <https://doi.org/10.3390/computers13030060>.
- [29]. Saadouni, R., Gherbi, C., Aliouat, Z., Harbi, Y., and Khacha, A. (2024) 'Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: A systematic review of the literature', *Cluster Computing*. <https://doi.org/10.1007/s10586-024-04388-5>.
- [30]. Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., and Gasmi, K. (2023) 'Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity', *Applied Sciences*, 13(13), p. 7507. <https://doi.org/10.3390/app13137507>.
- [31]. Alotaibi, A. and Rassam, M.A. (2023) 'Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense', *Future Internet*, 15(2), p. 62. <https://doi.org/10.3390/fi15020062>.
- [32]. Sowmya, T. and Mary Anita, E.A. (2023) 'A comprehensive review of AI based intrusion detection system', pp. 100827–100827. <https://doi.org/10.1016/j.measen.2023.100827>.
- [33]. Chan, K.Y. et al. (2023) 'Deep neural networks in the cloud: Review, applications, challenges and research directions', *Neurocomputing*, 545, p. 126327. <https://doi.org/10.1016/j.neucom.2023.126327>.
- [34]. Bałdyga, M., Barański, K., Belter, J., Kalinowski, M., and Weichbroth, P. (2024) 'Anomaly detection in railway sensor data environments: State-of-the-art methods and empirical performance evaluation', *Sensors*, 24(8), pp. 2633–2633. <https://doi.org/10.3390/s24082633>.
- [35]. Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., and Gasmi, K. (2023) 'Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity', *Applied Sciences*, 13(13), p. 7507. <https://doi.org/10.3390/app13137507>.
- [36]. Hernandez-Jaimes, M.L., Martinez-Cruz, A., Ramirez-Gutiérrez, K.A., and Feregrino-Uribe, C. (2023) 'Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures', *Internet of Things*, 23, p. 100887. <https://doi.org/10.1016/j.iot.2023.100887>.
- [37]. Saadouni, R., Gherbi, C., Aliouat, Z., Harbi, Y., and Khacha, A. (2024) 'Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: A systematic review of the literature', *Cluster Computing*. <https://doi.org/10.1007/s10586-024-04388-5>.
- [38]. Katarya, R. (2022) 'Towards the significance of taxi recommender systems in smart cities', *Concurrency and Computation: Practice and Experience*, 35(2). <https://doi.org/10.1002/cpe.7475>.
- [39]. Belay, M.A., Blakseth, S.S., Rasheed, A. and Salvo Rossi, P. (2023) 'Unsupervised anomaly detection for IoT-based multivariate time series: existing solutions, performance analysis and future directions', *Sensors*, 23(5), p. 2844. <https://doi.org/10.3390/s23052844>.
- [40]. Santhosh Kumar, S.V.N., Selvi, M. and Kannan, A. (2023) 'A comprehensive survey on machine learning-based intrusion detection systems for secure communication in Internet of Things', *Computational Intelligence and Neuroscience*, 2023, pp. 1–24. <https://doi.org/10.1155/2023/8981988>.
- [41]. Abdulganiyu, O.H., Ait Tchakoucht, T. and Saheed, Y.K. (2023) 'A systematic literature review for network intrusion detection system (IDS)', *International Journal of Information Security*. <https://doi.org/10.1007/s10207-023-00682-2>.
- [42]. Solaas, N., Tuptuk, and Mariconti, E. (2024) 'Systematic review: anomaly detection in connected and autonomous vehicles', *arXiv* (Cornell University). <https://doi.org/10.48550/arxiv.2405.02731>.

- [43]. Santhosh Kumar, S.V.N., Selvi, M. and Kannan, A. (2023) 'A comprehensive survey on machine learning-based intrusion detection systems for secure communication in Internet of Things', *Computational Intelligence and Neuroscience*, 2023, pp. 1–24. <https://doi.org/10.1155/2023/8981988>.
- [44]. Heidari, A. and Jabraeil Jamali, M.A. (2022) 'Internet of Things intrusion detection systems: a comprehensive review and future directions', *Cluster Computing*. <https://doi.org/10.1007/s10586-022-03776-z>.
- [45]. Shaik, T. et al. (2023) 'Remote patient monitoring using artificial intelligence: current state, applications, and challenges', *WIREs Data Mining and Knowledge Discovery*, 13(2). <https://doi.org/10.1002/widm.1485>.
- [46]. Mvula, P.K., Branco, P., Jourdan, G.-V. and Viktor, H.L. (2024) 'A survey on the applications of semi-supervised learning to cyber-security', *ACM Computing Surveys*. <https://doi.org/10.1145/3657647>.
- [47]. Liu, J. et al. (2024) 'Networking systems for video anomaly detection: a tutorial and survey', *arXiv* (Cornell University). <https://doi.org/10.48550/arxiv.2405.10347>.
- [48]. Le, M. et al. (2023) 'Applications of distributed machine learning for the Internet-of-Things: a comprehensive survey', *arXiv* (Cornell University). <https://doi.org/10.48550/arxiv.2310.10549>.
- [49]. Mohtasham-Amiri, Z., Heidari, A., Navimipour, N.J., Ünal, M. and Mousavi, A. (2023) 'Adventures in data analysis: a systematic review of deep learning techniques for pattern recognition in cyber-physical-social systems', *Multimedia Tools and Applications*. <https://doi.org/10.1007/s11042-023-16382-x>.
- [50]. Sun, M., He, L. and Zhang, J. (2022) 'Deep learning-based probabilistic anomaly detection for solar forecasting under cyberattacks', *International Journal of Electrical Power & Energy Systems*, 137, p. 107752. <https://doi.org/10.1016/j.ijepes.2021.107752>.
- [51]. Thakur, N., Nagrath, P., Jain, R., Saini, D., Sharma, N. and Jude Hemanth, D. (2021) 'Artificial intelligence techniques in smart cities surveillance using UAVs: a survey', pp. 329–353. [https://doi.org/10.1007/978-3-030-72065-0\\_18](https://doi.org/10.1007/978-3-030-72065-0_18).
- [52]. Islam, Md.M., Nooruddin, S., Karray, F. and Muhammad, G. (2022) 'Human activity recognition using tools of convolutional neural networks: a state of the art review, data sets, challenges, and future prospects', *Computers in Biology and Medicine*, 149, p. 106060. <https://doi.org/10.1016/j.compbiomed.2022.106060>.
- [53]. Aouedi, O., Piamrat, K. and Parrein, B. (2022) 'Intelligent traffic management in next-generation networks', *Future Internet*, 14(2), p. 44. <https://doi.org/10.3390/fi14020044>.
- [54]. Tama, B.A., Lee, S.Y. and Lee, S. (2022) 'A systematic mapping study and empirical comparison of data-driven intrusion detection techniques in industrial control networks', *Archives of Computational Methods in Engineering*, 29(7), pp. 5353–5380. <https://doi.org/10.1007/s11831-022-09767-y>.
- [55]. Alsoufi, M.A. et al. (2024) 'An anomaly intrusion detection systems in IoT based on autoencoder: a review', *Lecture Notes on Data Engineering and Communications Technologies*, pp. 224–239. [https://doi.org/10.1007/978-3-031-59707-7\\_20](https://doi.org/10.1007/978-3-031-59707-7_20).
- [56]. Mazhar, T. et al. (2023) 'Analysis of challenges and solutions of IoT in smart grids using AI and machine learning techniques: a review', *Electronics*, 12(1), p. 242. <https://doi.org/10.3390/electronics12010242>.
- [57]. Rao, P.M. and Deebak, B.D. (2022) 'Security and privacy issues in smart cities/industries: technologies, applications, and challenges', *Journal of Ambient Intelligence and Humanized Computing*. <https://doi.org/10.1007/s12652-022-03707-1>.
- [58]. Rafiq, I., Mahmood, A., Razzaq, S., Jafri, H.M. and Aziz, I. (2023) 'IoT applications and challenges in smart cities and services', *The Journal of Engineering*, 2023(4). <https://doi.org/10.1049/tje2.12262>.
- [59]. Gugueoth, V., Safavat, S. and Shetty, S. (2023) 'Security of Internet of Things (IoT) using federated learning and deep learning - recent advancements, issues and prospects', *ICT Express*. <https://doi.org/10.1016/j.icte.2023.03.006>.
- [60]. Javed, A.R., Ahmed, W., Pandya, S., Maddikunta, P.K.R., Alazab, M. and Gadekallu, T.R. (2023) 'A survey of explainable artificial intelligence for smart cities', *Electronics*, 12(4), p. 1020. <https://doi.org/10.3390/electronics12041020>.
- [61]. Kaur, B. et al. (2023) 'Internet of Things (IoT) security dataset evolution: challenges and future directions', *Internet of Things*, p. 100780. <https://doi.org/10.1016/j.iot.2023.100780>.
- [62]. Mazhar, T. et al. (2023) 'Analysis of IoT security challenges and its solutions using artificial intelligence', *Brain Sciences*, 13(4), p. 683. <https://doi.org/10.3390/brainsci13040683>.
- [63]. Ghaffari, A., Jelodari, N., pouralish, S., derakhshanfard, N. and Arasteh, B. (2024) 'Securing Internet of Things using machine and deep learning methods: a survey', *Cluster Computing*. <https://doi.org/10.1007/s10586-024-04509-0>.
- [64]. Omrany, H., Al-Obaidi, K.M., Hossain, M., Alduais, N.A.M., Al-Duais, H.S. and Ghaffarianhoseini, A. (2024) 'IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction', *Discover Cities*, 1(1). <https://doi.org/10.1007/s44327-024-00002-w>.



- [65]. Kumar, D., Pawar, P., Gonaygunta, H. and Singh, S. (2023) 'Impact of federated learning on industrial IoT - a review', *International Journal of Advanced Research in Computer and Communication Engineering*, 13(1). <https://doi.org/10.17148/ijarcce.2024.13105>.
- [66]. Qiu, Y., Ma, L. and Priyadarshi, R. (2024) 'Deep learning challenges and prospects in wireless sensor network deployment', *Archives of Computational Methods in Engineering*. <https://doi.org/10.1007/s11831-024-10079-6>.
- [67]. Belghachi, M. (2023) 'A review on explainable artificial intelligence methods, applications, and challenges', *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, 11(4), pp. 1007–1024. <https://doi.org/10.52549/ijeei.v11i4.5151>.
- [68]. Pawlicki, M., Pawlicka, A., Kozik, R. and Choraś, M. (2024) 'Advanced insights through systematic analysis: mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity', *Neurocomputing*, p. 127759. <https://doi.org/10.1016/j.neucom.2024.127759>.
- [69]. Khazane, H., Ridouani, M., Salahdine, F. and Kaabouch, N. (2024) 'A holistic review of machine learning adversarial attacks in IoT networks', *Future Internet*, 16(1), p. 32. <https://doi.org/10.3390/fi16010032>.
- [70]. Bechar, A., Elmir, Y., Himeur, Y., Medjoudj, R. and Amira, A. (2024) 'Federated and transfer learning for cancer detection based on image analysis', *arXiv* (Cornell University). <https://doi.org/10.48550/arxiv.2405.20126>.
- [71]. Zhang, C., Yang, S., Mao, L. and Ning, H. (2024) 'Anomaly detection and defense techniques in federated learning: a comprehensive review', *Artificial Intelligence Review*, 57(6). <https://doi.org/10.1007/s10462-024-10796-1>.
- [72]. Yan, R. et al. (2024) 'Transfer learning for prognostics and health management: advances, challenges, and opportunities', *Journal of Dynamics, Monitoring and Diagnostics*. <https://doi.org/10.37965/jdmd.2024.530>.

#### BIOGRAPHIES OF AUTHORS :

	<p><b>Mr. Zafar Iqbal</b> is currently serving as an <b>Manager Information Security at Ufone</b>, a leading telecommunications company in Pakistan. With over <b>8 years of experience</b> in the industry, he has played a pivotal role in various projects that enhance customer experience and optimize network performance. Zafar holds a <b>Master's degree in Information Security</b> from Riphah University, where he graduated with distinction. His areas of expertise include <b>network security, data protection, and cybersecurity incident response</b>. Throughout his career, Zafar has contributed significantly to Ufone's strategic initiatives, leading teams to implement innovative solutions that address evolving market demands. In addition to his technical prowess, Zafar is dedicated to <b>mentoring young professionals</b> in the industry, having successfully guided several interns and new hires during their transition into the corporate world. His efforts have been recognized through various <b>employee excellence awards</b>, highlighting his contributions to the company's success. Outside of work, Zafar is passionate about <b>technology education</b> and actively participation in community outreach.</p>
	<p><b>Dr. Ahthasham Sajid</b>    is an HEC Approved Supervisor and currently working as "<b>Assistant Professor</b>" in Department of Cyber Security in Riphah Institute of System Engineering, Riphah International University Islamabad Pakistan, previously I served as Assistant Professor under department of Computer Science in BUIITEMS Quetta from 2010 to 2023. I have also served as HOD for 5 years; I have done PhD in Computer Science in year 2020 from SZABIST, Islamabad Pakistan. My areas of interest are Wireless &amp; Sensor Networks (VANET, MANETS, and UAVs), and Cyber Security. I have <b>19 SCI, 14 SCOPUS / ESCI indexed, 20 HEC Recognized Journal, 06 International and 02 National Conference Proceedings Publications. 03 Book Chapters Publications</b>. I have successfully supervised 7 MS thesis and am currently supervising 01 PhD thesis. I have been serving as reviewer for IEEE Access, Willey Software and Practice, MDPI, Springer and other well-renowned journals. I have been awarded as best faculty member award in 2010 at BUIITEMS and also got merit scholarship in fall 2002 and Spring 2003 semester during my BCS (H) degree at Iqra University Quetta. He can be contacted at email: <a href="mailto:ahthasham.sajid@riphah.edu.pk">ahthasham.sajid@riphah.edu.pk</a>.</p>

	<p><b>Mr. Muhammad Nauman Zakki</b> is Certified Information Systems Auditor and Certified in Governance of Enterprise IT <b>from ISACA</b> currently working with <b>5 years of experience</b> in the field. I completed my bachelors from UET Lahore in Electrical Engineering (Computing) and secured <b>Gold Medal</b> in Masters <b>program of Information Security</b> <u>from Riphah International University Islamabad</u>, an HEC approved institution, with a particular focus on <b>data privacy and cybersecurity threats</b>. I am currently serving in a <b>public sector</b> as Asst. Director Governance, Risk and Compliance (GRC) . My areas of expertise include data protection, risk assessments, compliance with international Standards like HITRUST, HIPPA, ISO27001 etc., and the development of robust <b>cybersecurity frameworks and Information Security policy Drafting</b> to safeguard organizations from cyber threats. In my current role, I have successfully formulated and implemented comprehensive cybersecurity policies, audits and frameworks ensuring compliance with international standards. I have contributed to various research initiatives focused on <b>cybersecurity risk management and Governance</b> and have written several published journals as well. My goal is to continue advancing in the field by pursuing innovative solutions to modern cybersecurity challenges, ensuring that organizations are both <b>secure and resilient</b> in the face of potential cyber threats.</p>
	<p><b>Dr. Adeel Zafar</b> is currently working as “<b>Associate Professor</b>” / <b>Head of Department</b> in Riphah Institute of System Engineering, Riphah International University Islamabad Pakistan, He can be contacted at email: <a href="mailto:adeel.zafar@riphah.edu.pk">adeel.zafar@riphah.edu.pk</a> .</p>
	<p><b>Mr. Arshad Mehmood</b> is MS in Information Security and a Master's in Computer Science. My research interests lie in the fields of information security, blockchain technology, and cybersecurity. I am particularly passionate about exploring industry-level solutions for blockchain security and the application of smart contracts to enhance the security of IoT devices. Currently, I am working as Research Assistant in Riphah International University, Islamabad, Pakistan.</p>