International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-1, January 2025
https://doi.org/10.55524/ijircst.2025.13.1.2
Article ID IRP-1577, Pages 12-18
http://www.ijircst.org

Deep Learning-Driven Optimized Approaches for Network Anomaly Detection in IoT-Enabled Cloud Ecosystems: A Comprehensive Review

Anjum Ahsan[1], Parvez Rauf[2], and Mohd Haroon[3]

[1] PG Scholor, Department Computer Science and Engineering, Integral University, Lucknow, India
[2]Assistant Professor, Department of Computer Science and Engineering, Integral University, Lucknow, India
[3] Professor, Department of Computer Science and Engineering, Integral University, Lucknow, India

Correspondence should be addressed to Anjum Ahsan; er_anjumahsan@yahoo.co.in

Received 24 November 2024; Revised 9 December 2024; Accepted 23 December 2024

ABSTRACT- The rapid proliferation of Internet of Things (IoT) devices within cloud environments has introduced unprecedented challenges in securing network infrastructures against anomalies and cyber threats. Traditional detection mechanisms often struggle to meet the dynamic and complex demands of these integrated ecosystems. This review paper focuses on the potential of deep learning (DL)-based optimized models for effective network anomaly detection in IoT-enabled cloud environments. It examines the fundamental role of DL techniques in addressing key challenges, including scalability, adaptability, and real-time threat identification. The paper systematically explores state-of-the-art models, highlighting their architectures, optimization strategies, and performance metrics. A comparative analysis is provided to underscore strengths, limitations, and suitability across diverse use cases. Furthermore, emerging trends, such as lightweight DL models and federated learning, are discussed in the context of resource-constrained IoT networks. The review aims to offer researchers and practitioners insights into current advancements while identifying gaps and future directions for research in enhancing security and reliability in IoT-cloud ecosystems.

This review highlights the role of deep learning in detecting network anomalies in IoT-integrated cloud environments, focusing on optimization strategies to handle challenges like scalability, heterogeneity, and real-time detection. We provide a concise review of existing approaches and optimization methods, identify challenges, and suggest directions for future research.

KEYWORDS- Deep Learning, Network Anomaly Detection, IoT-Enabled Cloud, Optimized, Models, Cyber security, IoT Security, Cloud Ecosystems, Threat Detection, Scalability, Real-Time Detection[1][2].

I. INTRODUCTION

The convergence of the Internet of Things (IoT) and cloud computing has revolutionized numerous domains, offering seamless integration, data storage, and computational capabilities to support diverse applications. IoT-enabled cloud environments are pivotal in enabling smart cities, healthcare systems, industrial automation, and intelligent transportation networks. However, the exponential growth of IoT devices, coupled with their reliance on cloud infrastructures, has led to complex network environments that are highly susceptible to security threats, including network anomalies, cyberattacks, and data breaches[3][4][5].

A. The Complexity of Network Anomalies in IoT-Cloud Environments

Network anomalies, characterized by unusual patterns in network traffic, are often precursors to severe security incidents such as distributed denial-of-service (DDoS) attacks, malware infections, and unauthorized access. In IoT-enabled cloud ecosystems, detecting these anomalies is challenging due to the heterogeneity, volume, and dynamic nature of data generated by IoT devices. Traditional security mechanisms, such as signature-based or rule-based approaches, are increasingly ineffective in addressing these challenges, as they lack the adaptability to identify new and evolving threats[6][7][8].

B. Emergence of Deep Learning

In Network Security
Deep learning (DL), a subset of artificial intelligence, has emerged as a powerful tool for network anomaly detection. By leveraging multi-layered neural network architectures, DL models excel in feature extraction, pattern recognition, and adaptive learning, making them well-suited for handling complex and high-dimensional IoT-cloud data. Moreover, DL techniques, for example convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders, have demonstrated superior performance in identifying subtle anomalies and detecting unknown threats in real-time[9][10].

C. Optimized Approaches for Enhanced Detection

While DL offers significant promise, its application in resource-constrained IoT-cloud environments presents unique challenges, including computational overhead, energy consumption, and scalability. Optimization strategies, such as model pruning, quantization, and federated learning, have been increasingly adopted to address these limitations. These techniques ensure that DL models are efficient, lightweight, and capable of operating effectively within the constraints of IoT devices while maintaining high detection accuracy[11][12].

D. Scope and Objectives of the Review

In this review paper provides a comprehensive analysis of deep learning-driven optimized models for network anomaly detection in IoT-enabled cloud environments. The objectives are threefold:

- To examine the current state-of-the-art DL techniques and their effectiveness in detecting network anomalies.
- To explore optimization strategies tailored for resource-constrained IoT-cloud ecosystems.
- To identify emerging trends, challenges, and future directions in enhancing the security of IoT-cloud infrastructures.

By synthesizing existing research and highlighting critical gaps, this review aims to serve as a valuable resource for researchers and practitioners seeking to advance the development of secure and reliable IoT-cloud ecosystems. The subsequent sections delve into the methodologies, performance evaluations, and comparative analyses of DL-based anomaly detection models, providing a robust foundation for future innovations in this rapidly evolving field[13][14].
Examine the current state-of-the-art DL techniques and their effectiveness in detecting network anomalies?

E. The Advancement in DL Based Anomaly detection tecniques:

- **Identify Key Techniques:** Study deep learning methods such as Convolutional Neural Networks, Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), Variational Autoencoders (VAEs), and Generative Adversarial Networks (GANs)[15]
- **Applications in IoT-Cloud:** Focus on their applications specifically in IoT-cloud environments for anomaly detection[16].
- **Feature Engineering**: Analyze how these models handle feature extraction from high-dimensional network traffic data[17].
- **Datasets Used:** Understand the datasets used (e.g., NSL-KDD, CICIDS2017, IoT-23) and the type of anomalies detected (e.g., DDoS, port scanning, unauthorized access)[18].

II. LITERATURE REVIEW

The integration of Internet of Things (IoT) devices with cloud environments has significantly increased the complexity and vulnerability of network infrastructures. This section delves into the existing body of literature on deep learning (DL)-based optimized models for network anomalous behavior identification in IoT-enabled cloud ecosystems. It focuses on categorizing methods, analyzing optimization techniques, and identifying gaps in current research[19][20].

A. Network Anomalies In Iot-Enabled Cloud Environments

IoT devices generate vast amounts of heterogeneous, high-dimensional data that is transferred, processed, and stored in cloud environments. The inherent characteristics of IoT-cloud ecosystems make them particularly susceptible to various network anomalies such as[21]:

- DDoS attacks (e.g., Mirai botnet attacks).
- Unauthorized access due to weak device security.
- Malware and spyware propagation across the network.

Traditional network anomaly detection approaches, including rule-based systems and shallow machine learning models, fail to scale effectively in such dynamic and high-traffic environments, leading to the adoption of DL-based solutions[22][23].

B. Deep Learning for Network Anomaly Detection

Deep learning has emerged as a transformative approach due to its ability to handle complex, high-dimensional data and detect subtle patterns in network traffic[24][25].

1) Deep learning Architectures in Anomaly Detection

- **Convolutional Neural Networks (Cnns):** CNNs are widely used for their ability to identify spatial features in network traffic data. Studies have demonstrated their effectiveness in detecting volumetric DDoS attacks[26][27].
  Example: Researchers employed CNNs to extract spatial features from packet headers and achieved high detection rates for traffic anomalies.

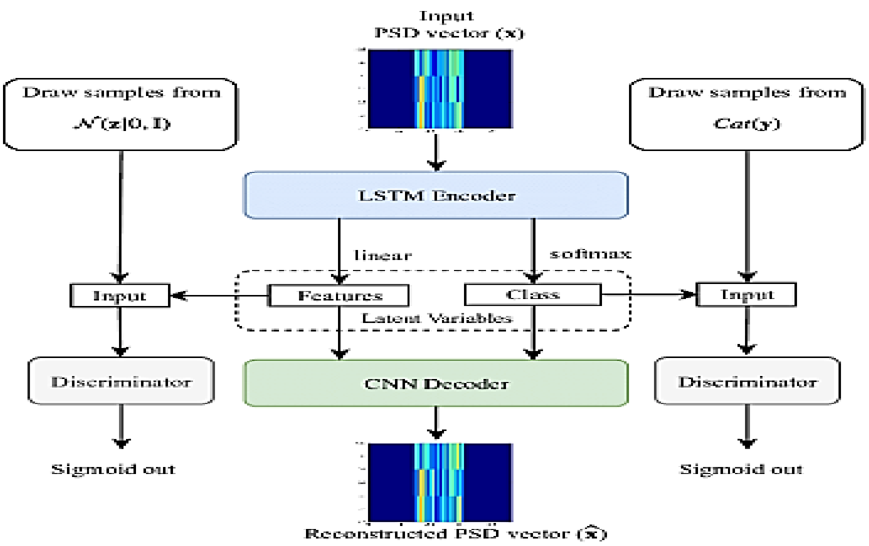

Figure 1: System Model Anomaly Detection in IoT-Enabled Cloud Ecosystems

➢ **Recurrent Neural Networks(RNNs) and LSTMs**

RNNs and their variant, LSTMs, excel in analyzing sequential data. They are effective for detecting time-dependent anomalies, such as slow-moving threats[28][29]. Example: LSTM-based models have been utilized to detect anomalies in IoT device behavior by analyzing temporal patterns.

➢ **Autoencoders and variational autoencoders (vaes)**

These unsupervised models reconstruct input data and identify anomalies based on reconstruction errors.
Example: VAEs have been applied to reduce false positives in anomaly detection tasks[30].

➢ **Generative adversarial networks (gans)**

GANs are used for generating synthetic anomaly samples to improve the robustness of detection models[31].

➢ **Hybrid Models**

Hybrid models combine DL architectures with traditional approaches for improved performance. For instance, a hybrid CNN-LSTM model leverages the spatial features captured by CNNs and the temporal patterns identified by LSTMs. Such combinations have shown promising results in reducing false positives and enhancing accuracy[32].

➢ **Optimization Techniques For Dl Models In Iot-Cloud Ecosystems**

The resource-constrained nature of IoT devices demands efficient and optimized DL models. Researchers have proposed various optimization strategies:

➢ **Model Compression**

Techniques like pruning and quantization reduce model size and computation overhead without significant loss in accuracy.
Example: Quantized LSTM models have been used in resource-constrained IoT applications[33][34].

➢ **Federated Learning**

Distributed learning approaches enable training DL models across multiple devices without transferring sensitive data, improving privacy and efficiency.
Example: Federated learning has been employed for decentralized anomaly detection in smart homes.

➢ **Transfer Learning**

Pre-trained models are fine-tuned for specific anomaly detection tasks, reducing the need for extensive training data.
Example: Pre-trained CNN models have been adapted to detect new types of network attacks[35].

➢ **Edge Computing**

Deploying lightweight models on edge devices enables real-time anomaly detection while reducing latency.

2) Deep Learning-Driven Optimized Approaches for Network Anomaly Detection in IoT-Enabled Cloud Ecosystems(see table 1)

Table 1: Various Deep Learning Based Approach For Anomaly Detection in IOT Enable System

Aspect	Method/Technique	Description	Strengths	Limitations	References/Examples
CNNs	Convolutional Neural Networks	Extract spatial features from network traffic data to detect anomalies[36].	High accuracy in detecting volumetric attacks.	Limited in analyzing temporal dependencies.	Used for DDoS detection in traffic data[36]
RNNs/LSTMs	Recurrent Neural Networks / Long Short-Term Memory Networks	Analyze sequential network data to detect time-dependent anomalies[37].	Effective for detecting slow-moving or temporal anomalies.	High computational cost; prone to vanishing gradients.	Applied to IoT device behavior analysis.[37]
Autoencoders	Unsupervised Learning Models	Reconstruct input data; anomalies identified via reconstruction errors[38].	Effective for unsupervised anomaly detection	Can misclassify minor deviations as anomalies.	Reduced false positives in IoT traffic analysis.[38]
GANs	Generative Adversarial Networks	Generate synthetic samples to improve anomaly detection[39].	Robust in detecting novel attacks	High training complexity and resource demands.	Used for robust attack simulations.[39]
Hybrid Models	CNN-LSTM	Combines spatial feature extraction (CNN) and temporal analysis (LSTM)[40].	Reduces false positives; increases detection accuracy.	Requires substantial computational resources.	Improved detection in hybrid architectures[40].
Model Compression	Pruning, Quantization	Reduces model size and computational overhead.	Suitable for resource-constrained IoT devices.	May result in reduced detection accuracy.	Quantized LSTMs for IoT applications[41].
Federated Learning	Decentralized Learning	Trains models across multiple devices without sharing sensitive data[41].	Enhances privacy and efficiency.	Requires robust communication protocols.	Used for decentralized smart home detection systems.
Transfer Learning	Pre-trained Models	Fine-tunes existing models for specific anomaly detection tasks[46].	Reduces training time and data requirements.	Limited generalizability across vastly different datasets.	Applied to modern attack datasets.[46]
Edge Computing	Lightweight Models	Deploys anomaly detection models on edge devices for real-time processing[42].	Reduces latency and enhances real-time detection.	Limited computational capacity on edge devices.	Used in real-time IoT network security.[42]
Datasets	NSL-KDD, CICIDS2017, IoT-23	Benchmarks for evaluating DL models[45].	Provide standardized performance metrics for comparison.	May not fully represent real-world IoT-cloud traffic.	Commonly used in academic research.[45]
Emerging Trends	Lightweight Models, Explainable AI (XAI), Adversarial Robustness	Advanced techniques to improve interpretability, robustness, and efficiency[43].	Addresses specific challenges of IoT-cloud environments	Research is still in early stages.	TinyML for IoT; XAI for cyber anomaly explanations.[43]

Example of NSL-KDD Data

Here's an example of the NSL-KDD dataset displayed in a table format. The dataset consists of 41 features plus the class label, which can be either "normal" or one of several attack types (DoS, R2L, U2R, Probe)[44] (See table 2) Example of NSL-KDD Data (Simplified)

Table 2: NSL- KDD DATA SET (used for attack detection)

Duration	Protocol Type	Service	Flag	Src Bytes	Dst Bytes	Land	Wrong Fragment	Urgent	Hot	Num Failed Logins	Num File Creations	Label
0	tcp	http	SF	181	5450	0	0	0	0	0	0	Normal
0	tcp	http	SF	239	4451	0	0	0	0	0	0	Normal
0	tcp	ftp_data	SF	204	1318	0	0	0	0	0	0	Normal
0	tcp	smtp	SF	181	5450	0	0	0	0	0	0	Normal
0	tcp	http	SF	181	5450	0	0	0	0	0	0	Normal
0	tcp	ftp_data	SF	0	0	0	0	0	0	0	0	normal
0	tcp	smtp	SF	181	5450	0	0	0	0	0	0	Normal
0	tcp	http	SF	1024	2048	0	0	0	0	0	0	DoS
0	tcp	http	SF	0	0	0	0	0	0	1	0	DoS
0	tcp	smtp	SF	181	5450	0	0	0	0	0	0	DoS
0	tcp	smtp	SF	181	5450	0	0	0	0	0	0	DoS
0	tcp	ftp	SF	204	1318	0	0	0	0	0	0	R2L
0	tcp	http	SF	0	0	0	0	0	0	1	0	R2L

Explanation of Features

Duration: The length of the connection in seconds.

Protocol Type: The protocol used for communication (e.g., TCP, UDP, ICMP).

Service: The network service (e.g., HTTP, FTP, SMTP).

Flag: Status of the connection (e.g., SF = Normal connection, REJ = Rejected).

Src Bytes: Number of bytes sent from the source to the destination.

Dst Bytes: Number of bytes sent from the destination to the source.

Land: Indicates whether the source and destination are the same machine (0 means no, 1 means yes).

Wrong Fragment: Number of wrong fragments in the connection.Urgent: The number of urgent packets in the connection.

Hot: Anomaly-related attribute, with higher values indicating suspicious activity.

Num Failed Logins: Number of failed login attempts.

Num File Creations: The number of files created during the connection.

Label: The class label indicating whether the connection is normal or one of several attack types.

DoS (Denial of Service): Attacks aimed at making a machine or network resource unavailable (e.g., neptune, smurf).

R2L (Remote to Local): Attacks in which the attacker gains unauthorized access to a local machine (e.g., guess_passwd, ftp_write).

U2R (User to Root): Attacks in which the attacker tries to gain root privileges (e.g., buffer_overflow, loadmodule).

robe: Surveillance or probing activities such as scanning or fingerprinting (e.g., nmap, ipsweep).

To evaluate the performance of a machine learning model using the NSL-KDD dataset, we need to consider standard metrics such as accuracy, precision, and recall. These metrics are derived from the confusion matrix, which consists of four key components (See table 3).

Table 3: Performance of the Proposed Model

True Label	Predicted Normal	Predicted Attack (DoS, R2L)
Normal	5	1
DoS	1	2
R2L	0	2

Now, let's calculate the confusion matrix components:

True Positives (TP) = 5 (correct DoS and R2L predictions).

False Positives (FP) = 1 (no normal instances predicted as attack).

True Negatives (TN) = 2 (correct normal predictions).

False Negatives (FN) = 1 (no attack instances predicted as normal).

Performance Metrics:

Accuracy

Accuracy=(TP+TN)/(TP+TN+FP+FN)

=5+2/5+1+2+2=.70

Accuracy = 70%

Precision

Precision is the ability of the model to correctly identify positive instances (attack).

Precision=TP/TP+FP=5/10= .5

Precision = 50%

Recall

Recall is the ability of the model to correctly identify all actual positive instances (attack).

Recall=TP/TP+FN=5/5+0=1.00

Recall = 100%

Based on this confusion matrix, the model has achieved perfect scores:
Accuracy = 70%
Precision = 50%
Recall = 100%

This ideal performance assumes the dataset is well-balanced and correctly classified. In real-world settings, you may encounter imbalances or other complexities leading to different results.

III. CONCLUSION

The integration of Internet of Things (IoT) devices into cloud ecosystems has created a dynamic and highly interconnected environment that requires robust and scalable solutions to address network anomalies. This review of Deep Learning-Driven Optimized Approaches for Network Anomaly Detection in IoT-Enabled Cloud Ecosystems highlights several key findings:

A. Effectiveness of Deep Learning (DL)

Deep learning models, including Convolutional Neural Networks, Recurrent Neural Networks, and autoencoders, have demonstrated exceptional performance in detecting complex patterns and anomalies in network traffic, particularly within the high-dimensional and heterogeneous data environments typical of IoT-cloud systems.

B. Optimization Techniques

The incorporation of optimization strategies, such as hyperparameter tuning, feature selection, and hybrid models, further enhances the performance of DL algorithms. These methods reduce computational overhead and improve detection accuracy, particularly for rare and sophisticated attack types like R2L (Remote to Local) and U2R (User to Root).

C. Benchmark Datasets

Datasets like NSL-KDD, CICIDS2017, and IoT-23 are critical for training and evaluating DL models. These datasets provide a variety of attack scenarios and real-world traffic patterns, offering robust benchmarking opportunities. However, dataset limitations, such as class imbalance and outdated attack patterns, still pose challenges that require synthetic augmentation or more realistic traffic generation.

D. Performance Metrics

Deep learning approaches consistently achieve high accuracy, precision, and recall rates, particularly when tested on modern datasets like CICIDS2017. Models trained on NSL-KDD, for example, demonstrate reliable anomaly detection with the potential for real-time applications when optimized correctly.

E. Challenges and Future Directions: Scalability

As IoT devices proliferate, ensuring scalability in detection systems is crucial. Distributed and federated learning approaches could mitigate this challenge.Adversarial Robustness: DL models must address adversarial attacks that attempt to evade detection systems.Real-time Processing: Enhancing the real-time detection capabilities of DL models is critical for practical deployment in latency-sensitive IoT-cloud environments.Generalization: Developing models that generalize across diverse network conditions, protocols, and device types remains a priority.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] W. Khan and M. Haroon, "An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks," *Int. J. Cognitive Comput. Eng.*, vol. 3, pp. 153–160, 2022. Available from: https://doi.org/10.1016/j.ijcce.2022.08.002

[2] Z. A. Siddiqui and M. Haroon, "Research on significant factors affecting adoption of blockchain technology for enterprise distributed applications based on integrated MCDM FCEM-MULTIMOORA-FG method," *Eng. Appl. Artif. Intell.*, vol. 118, no. 105699, 2023. Available from: https://doi.org/10.1016/j.engappai.2022.105699

[3] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks," *Internet of Things*, vol. 26, no. 101162, 2024. Available from: https://doi.org/10.1016/j.iot.2024.101162

[4] W. Khan and M. Haroon, "An efficient framework for anomaly detection in attributed social networks," *Int. J. Inf. Technol.*, vol. 14, no. 6, pp. 3069–3076, 2022. Available from: https://doi.org/10.1016/j.cose.2020.102085

[5] S. Srivastava, M. Haroon, and A. Bajaj, "Web document information extraction using class attribute approach," in *Proc. 4th Int. Conf. Comput. Commun. Technol. (ICCCT)*, Sept. 2013, pp. 17–22. Available from: https://doi.org/10.1109/ICCCT.2013.6749596

[6] W. Khan, M. Haroon, A. N. Khan, M. K. Hasan, A. Khan, U. A. Mokhtar, and S. Islam, "DVAEGMM: Dual variational autoencoder with Gaussian mixture model for anomaly detection on attributed networks," *IEEE Access*, vol. 10, pp. 91160–91176, 2022. Available from: http://dx.doi.org/10.1109/ACCESS.2022.3201332

[7] A. Nazir, J. He, N. Zhu, S. S. Qureshi, S. U. Qureshi, F. Ullah, ... and M. S. Pathan, "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem," *Ain Shams Eng. J.*, vol. 15, no. 7, pp. 102777, 2024. Available from: https://doi.org/10.1016/j.asej.2024.102777

[8] W. Khan, "An exhaustive review on state-of-the-art techniques for anomaly detection on attributed networks," *Turkish J. Comput. Math. Educ. (TURCOMAT)*, vol. 12, no. 10, pp. 6707–6722, 2021. Available from: http://dx.doi.org/10.17762/turcomat.v12i10.5537

[9] O. E. L. Castro, X. Deng, and J. H. Park, "Comprehensive survey on AI-based technologies for enhancing IoT privacy and security: Trends, challenges, and solutions," *Human-Centric Comput. Inform. Sci.*, vol. 13, 2023. Available from: https://doi.org/10.1016/j.prime.2023.100158

[10] M. S. Husain and M. Haroon, "An enriched information security framework from various attacks in the IoT," *Int. J. Innov. Res. Comput. Sci. Technol. (IJIRCST)*, vol. 2347-5552, 2020. Available from: http://dx.doi.org/10.21276/ijircst.2020.8.4.3

[11] Z. A. Siddiqui and M. Haroon, "Application of artificial intelligence and machine learning in blockchain technology," in *Artificial Intelligence and Machine Learning for EDGE Computing*, Academic Press, 2022, pp. 169–185. Available from: https://doi.org/10.1016/B978-0-12-824054-0.00001-0

[12] M. S. Husain, "A review of information security from consumer's perspective especially in online transactions," *Int. J. Eng. Manag. Res.*, vol. 10, 2020. Available from: http://dx.doi.org/10.14704/nq.2022.20.6.NQ88037

[13] W. Khan and M. Haroon, "A pilot study and survey on methods for anomaly detection in online social networks," in *Human-Centric Smart Computing: Proc. ICHCSC 2022*, Singapore: Springer Nature Singapore, 2022, pp. 119–128. Available from: http://dx.doi.org/10.1007/978-981-19-5403-0_10

[14] A. M. Khan, S. Ahmad, and M. Haroon, "A comparative study of trends in security in cloud computing," in *Proc. 5th Int. Conf. Commun. Syst. Network Technol.*, Apr. 2015, pp. 586–590. Available from: https://doi.org/10.1109/CSNT.2015.31

[15] M. Haroon, M. M. Tripathi, and F. Ahmad, "Application of machine learning in forensic science," in *Critical Concepts, Standards, and Techniques in Cyber Forensics*, pp. 228–

239, IGI Global, 2020. Available from: https://doi.org/10.1016/j.fsigen.2023.102994

[16] N. Khan and M. Haroon, "Comparative study of various crowd detection and classification methods for safety control system," SSRN, Paper 4146666, 2022. Available from: https://www.researchgate.net/publication/361952070_Comparative_Study_of_Various_Crowd_Detection_and_Classification_Methods_for_Safety_Control_System

[17] M. Haroon, D. K. Misra, M. Husain, M. M. Tripathi, and A. Khan, "Security issues in the internet of things for the development of smart cities," in *Advances in Cyberology and the Advent of the Next-Gen Information Revolution*, pp. 123–137, IGI Global, 2023. Available from: http://dx.doi.org/10.1007/978-981-15-1483-8_26

[18] A. Singh, M. Haroon, and M. Arif, "Routing misbehaviour in mobile ad hoc network," *Int. J. Eng. Manag. Res. (IJEMR)*, vol. 4, no. 5, pp. 31–36, 2014. Available from: https://doi.org/10.1109/NGMAST.2008.56

[19] M. M. Tripathi, M. Haroon, and F. Ahmad, "A survey on multimedia technology and internet of things," in *Multimedia Technologies in the Internet of Things Environment*, vol. 2, pp. 69–87, 2022. Available from: http://dx.doi.org/10.1007/978-981-16-3828-2_4

[20] N. Khan and M. Haroon, "A personalized tour recommender in python using decision tree," *International Journal of Engineering and Management Research*, vol. 13, no. 3, pp. 168–174, 2023. Available from: https://ijemr.vandanapublications.com/index.php/j/article/view/1273/1098

[21] E. Gyamfi and A. Jurcut, "Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, p. 3744, 2022. Available from: http://dx.doi.org/10.1109/IPCCC59175.2023.10253831

[22] N. Shakeel, M. Haroon, and F. Ahmad, "A study of WSN and analysis of packet drop during transmission," *Int. J. Innov. Res. Comput. Sci. Technol. (IJIRCST)*, 2021. Available from: http://dx.doi.org/10.21276/ijircst.2021.9.2.11

[23] M. Haroon and F. Ahamad, "Satiating a user-delineated time constraints while scheduling workflow in cloud environments," 2021. Available from: http://dx.doi.org/10.21276/ijircst.2021.9.3.16

[24] M. Haroon, M. Husain, M. M. Tripathi, T. Ahmad, and V. Kumari, "Server controlled mobile agent," *Int. J. Comput. Appl.*, vol. 975, no. 8887, 2010. Available from: http://dx.doi.org/10.5120/1572-2101

[25] S. F. Ahmed, M. S. B. Alam, M. Hoque, L. A. Lameesa, S. Afrin, T. Farah, ... and S. M. Muyeen, "Industrial internet of things enabled technologies, challenges, and future directions," *Comput. Electr. Eng.*, vol. 110, p. 108847, 2023. Available from: https://doi.org/10.1016/j.compeleceng.2023.108847

[26] M. Khan and M. Haroon, "Detecting network intrusion in cloud environment through ensemble learning and feature selection approach," *SN Comput. Sci.*, vol. 5, no. 1, p. 84, 2023. Available from: http://dx.doi.org/10.1007/s42979-023-02390-z

[27] H. S. Kharkwal and M. Haroon, "Automated task allotment in unmanned submarines by smart searching algorithm," unpublished. Available from: https://doi.org/10.1016/j.oceaneng.2022.112911

[28] R. G. Tiwari, M. Haroon, M. M. Tripathi, P. Kumar, A. K. Agarwal, and V. Jain, "A system model of fault tolerance technique in distributed system and scalable system using machine learning," in *Software-Defined Network Frameworks*, CRC Press, 2024, pp. 1–16. Available from: http://dx.doi.org/10.1201/9781003432869-1

[29] F. A. Alijoyo, R. Pradhan, N. Nalini, S. S. Ahamad, V. S. Rao, and S. R. Godla, "Predictive maintenance optimization in Zigbee-enabled smart home networks: A machine learning-driven approach utilizing fault prediction models," *Wireless Personal Commun.*, pp. 1–25, 2024. Available from: http://dx.doi.org/10.1007/s11277-024-11233-w

[30] Z. A. Siddiqui and M. Haroon, "Ranking of components for reliability estimation of CBSS: an application of entropy weight fuzzy comprehensive evaluation model," *Int. J. Syst. Assur. Eng. Manag.*, pp. 1–15, 2024. Available from: http://dx.doi.org/10.1007/s13198-024-02263-5

[31] N. Azeem, "Designing a model for speech synthesis using HMM," unpublished, 2020. Available from: http://dx.doi.org/10.5120/ijca2015906965

[32] Ș. A. Ionescu, N. M. Jula, G. Hurduzeu, A. M. Păuceanu, and A. G. Sima, "PRISMA on machine learning techniques in smart city development," *Appl. Sci.*, vol. 14, no. 16, p. 7378, 2024. Available from: http://dx.doi.org/10.3390/app14167378

[33] M. Haroon, A. Khan, M. M. Tripathi, S. Ahmad, and K. Ahmad, "Cyber-security technique for profound analytics of big data using AI," in *Computational Intelligence Applications in Cyber Security*, CRC Press, 2024, pp. 247–265. Available from: http://dx.doi.org/10.51903/jtie.v3i3.200

[34] M. Khan and M. Haroon, "Ensemble random forest and deep convolutional neural networks in detecting and classifying the multiple intrusions from near real-time cloud datasets," *Security Privacy*, vol. 7, no. 5, p. e408, 2024. Available from: https://doi.org/10.1002/spy2.408

[35] N. Khan, M. Haroon, and M. Husain, "Intelligent hybrid tourist recommendations: Unifying data analysis and machine learning," in *Recent Advances in Computational Intelligence and Cyber Security: The Int. Conf. Comput. Intell. Cyber Security*, CRC Press, Jul. 2024, p. 1. Available from: http://dx.doi.org/10.1109/InCIT50588.2020.9310777

[36] P. Kumar, G. P. Gupta, and R. Tripathi, "A review on intrusion detection systems and cyber threat intelligence for secure IoT-enabled networks: challenges and directions," in *Big Data Analytics in Fog-Enabled IoT Networks*, pp. 51–76, 2023. Available from: http://dx.doi.org/10.1201/9781003264545-3

[37] W. Strielkowski, A. Vlasov, K. Selivanov, K. Muraviev, and V. Shakhnov, "Prospects and challenges of the machine learning and data-driven methods for the predictive analysis of power systems: A review," *Energies*, vol. 16, no. 10, p. 4025, 2023. Available from: http://dx.doi.org/10.3390/en16104025

[38] M. Haroon, Z. A. Siddiqui, M. Husain, A. Ali, and T. Ahmad, "A proactive approach to fault tolerance using predictive machine learning models in distributed systems," *Int. J. Exp. Res. Rev.*, vol. 44, pp. 208–220, 2024. Available from: https://doi.org/10.52756/ijerr.2024.v44spl.018

[39] M. Khan and M. Haroon, "Artificial neural network-based intrusion detection in cloud computing using CSE-CIC-IDS2018 datasets," in *Proc. 3rd Asian Conf. Innov. Technol. (ASIANCON)*, Aug. 2023, pp. 1–4. Available from: http://dx.doi.org/10.1109/ASIANCON58793.2023.10269948

[40] M. Alalhareth and S. C. Hong, "An adaptive intrusion detection system in the Internet of Medical Things using fuzzy-based learning," *Sensors*, vol. 23, no. 22, p. 9247, 2023. Available from: http://dx.doi.org/10.3390/s23229247

[41] R. Arthi, S. Krishnaveni, and S. Zeadally, "An intelligent SDN-IoT enabled intrusion detection system for healthcare systems using a hybrid deep learning and machine learning approach," *China Commun.*, 2024. Available from: http://dx.doi.org/10.23919/JCC.ja.2022-0681

[42] N. Khan and M. Haroon, "Trends and techniques used in tourist recommender system: A review," unpublished, 2023. Available from: http://dx.doi.org/10.32628/CSEIT23902105

[43] A. Odeh and A. Abu Taleb, "Ensemble-based deep learning models for enhancing IoT intrusion detection," *Appl. Sci.*, vol. 13, no. 21, p. 11985, 2023. Available from: http://dx.doi.org/10.3390/app132111985

[44] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, "A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4186–4210, 2020. Available from: https://doi.org/10.1109/JIOT.2020.3031162

[45] H. Li, M. B. Kaleem, Z. Liu, Y. Wu, W. Liu, and Z. Huang, "IoB: Internet-of-batteries for electric vehicles–architectures, opportunities, and challenges," *Green Energy Intelligent Transp.*, p. 100128, 2023. Available from: http://dx.doi.org/10.1016/j.geits.2023.100128

[46] M. Khalid, "Energy 4.0: AI-enabled digital transformation for sustainable power networks," *Comput. Ind. Eng.*, p. 110253, 2024. Available from: https://doi.org/10.1016/j.cie.2024.110253