Metaversalize

www.meta.reapress.com

Metaverse.Vol. 2, No. 1 (2025) 31–39.

Paper Type: Original Article

AI Enhanced Cybersecurity for Cloud-IoT Infrastructure in Smart Cities

G Dhvani Iyer*

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 2229031@kiit.ac.in.

Citation:

Received: 8 August 2024 *Revised: 27 November 2024* *Accepted: 2 January 2025*	Iyer, G. D. (2024). AI enhanced cybersecurity for cloud-IoT infrastructure in smart cities. *Metaversalize*, *2*(1), 31-39.

Abstract

As smart cities increasingly rely on Cloud-IoT infrastructure for connectivity and efficiency, they face escalating cyber threats. Traditional security methods are often inadequate against the dynamic cyber landscape. This paper explores the integration of Artificial Intelligence (AI) into cybersecurity frameworks to safeguard smart city infrastructures by leveraging predictive analysis, real-time threat detection, and adaptive response systems. We propose an AI-enhanced model that improves cyber-resilience for critical Cloud-IoT operations and examine case studies on smart city implementations.

Keywords: AI-enhanced cybersecurity, Cloud-IoT infrastructure, Smart cities, Anomaly detection, Machine learning and deep learning algorithms.

1 | Introduction

The evolution of smart cities relies heavily on integrating cloud and Internet of Things (IoT) technologies to enhance urban infrastructure, improve efficiency, and provide innovative services [1], [2]. However, as cloud-based IoT ecosystems grow in complexity, they become increasingly vulnerable to cyber threats that target interconnected networks, devices, and critical data flows. Traditional cybersecurity approaches are often inadequate to address these threats' dynamic and sophisticated nature. Therefore, Artificial Intelligence (AI) has emerged as a promising solution, with AI-enhanced security frameworks offering advanced capabilities to detect, respond, and mitigate cyber-attacks in real time [3–6].

AI in cybersecurity introduces intelligent algorithms that continuously learn from vast data sets, enabling predictive and adaptive defenses. In a smart city context, where IoT devices, sensors, and cloud servers are interconnected, AI-based systems can analyze behavior patterns and anomalies, which helps prevent potential intrusions and reduces response times to incidents. This proactive approach protects public infrastructure, personal data, and operational continuity. Furthermore, AI-enhanced cybersecurity can help manage the high

Corresponding Author: 2229031@kiit.ac.in

https://doi.org/10.22105/metaverse.v2i1.48

volume of network traffic characteristic of smart cities, ensuring that cloud-based systems operate securely and efficiently.

Implementing AI-driven cybersecurity within cloud-IoT infrastructures of smart cities presents unique challenges and opportunities. As AI systems require substantial computational power and a secure, resilient data architecture, integrating these with cloud and IoT infrastructures demands a tailored approach. This paper explores how AI-enhanced cybersecurity frameworks can be optimized for cloud-IoT environments, providing insights into their potential to safeguard smart cities against the evolving cyber threat landscape.

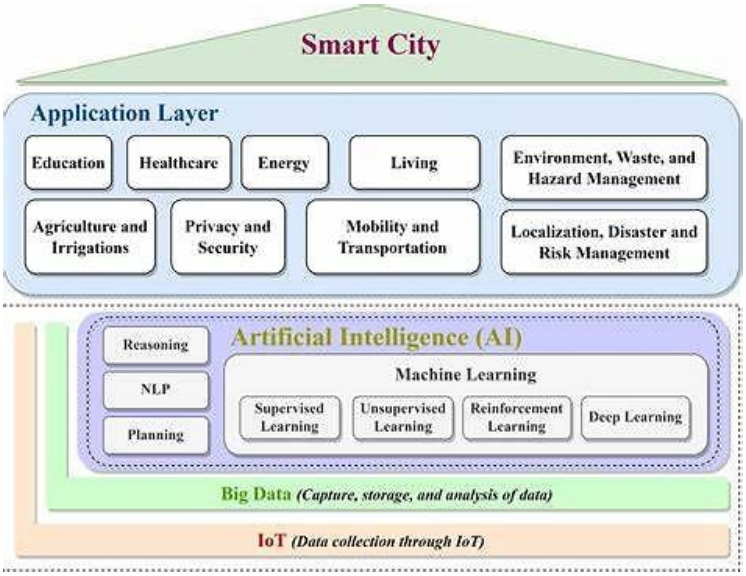

Fig. 1. Conceptual diagram of AI-enhanced cybersecurity in smart cities.

2 | Literature Review

2.1 | Overview of Cyber Threats in Cloud-IoT Systems

Cyber threats targeting Cloud-IoT infrastructures include Distributed Denial-Of-Service (DDoS) attacks, malware intrusions, and data breaches [7]. These attacks can disrupt city functions and compromise citizens' data.

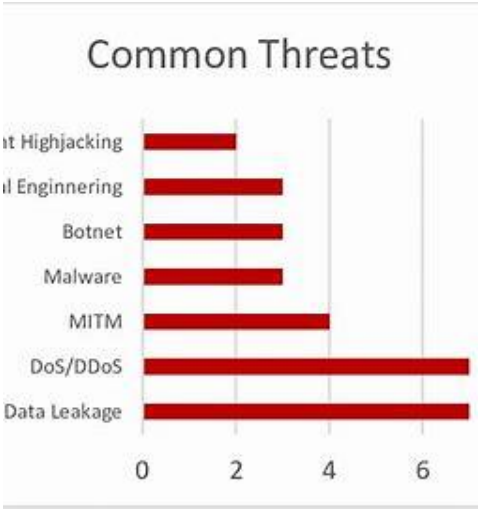

Fig. 2. Common cyber threats in Cloud-IoT systems.

2.1.1 | Traditional cybersecurity methods

Conventional cybersecurity techniques, including firewalls and signature-based malware detection, lack the adaptability to respond effectively to novel and complex cyber threats in real time.

2.1.2 | AI-driven cybersecurity solutions

AI-driven cybersecurity methods, including Machine Learning (ML) and Deep Learning (DL), enhance threat detection in Cloud-IoT infrastructures by analyzing large datasets for patterns, allowing systems to identify known and unknown risks. Key approaches include anomaly detection, which monitors real-time data for unusual activity; supervised learning, which classifies threats based on known examples; and unsupervised learning, which identifies hidden patterns in unlabeled data, making it ideal for emerging threats. These methods create adaptive, proactive security measures, enabling smart cities to safeguard against complex and evolving cyber risks effectively.

3 | Methodology

3.1 | Proposed AI-Enhanced Cybersecurity Model

Our proposed model combines AI algorithms with network anomaly detection to safeguard Cloud-IoT infrastructure in smart cities. We employed supervised learning techniques to train models on historical data, enabling proactive threat detection.

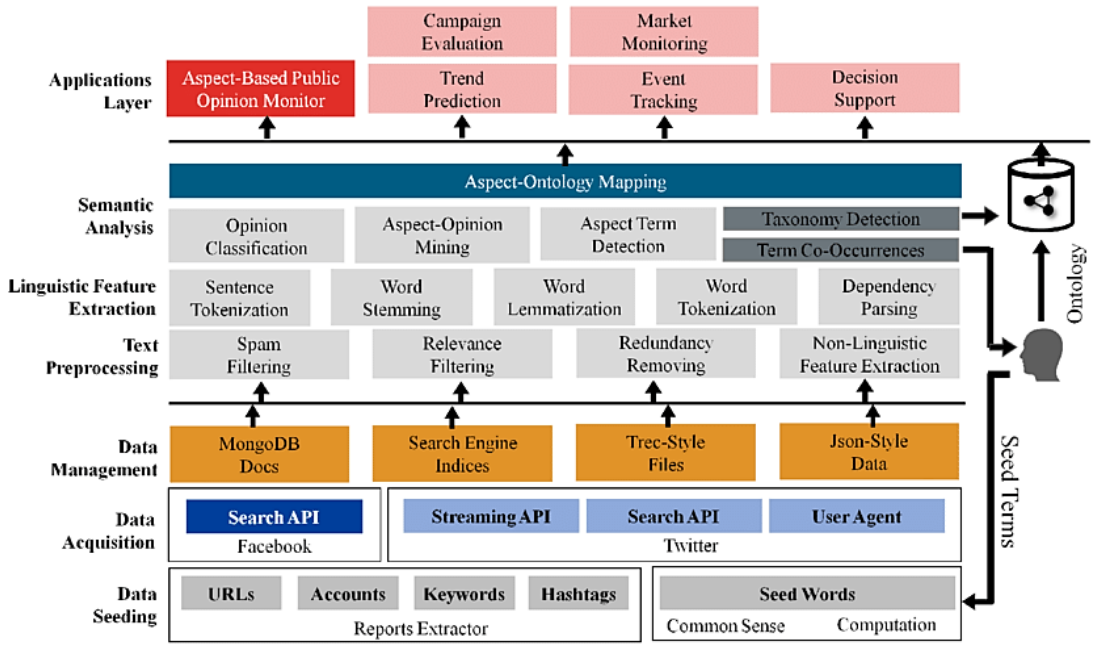

Fig. 3. Architecture diagram of the AI-enhanced cybersecurity model.

3.1.1 | Data collection

Data was collected from public IoT network logs and processed for training using feature extraction techniques.

3.1.2 | Algorithm design

Algorithms were designed to detect anomalies and identify intrusion patterns. Each component in the system was evaluated based on its performance in identifying and responding to security incidents.

3.2 | Implementation and Evaluation

We implemented the AI-enhanced model in a simulated smart city environment using real-time data from IoT devices and cloud systems to test its resilience to cyber threats.

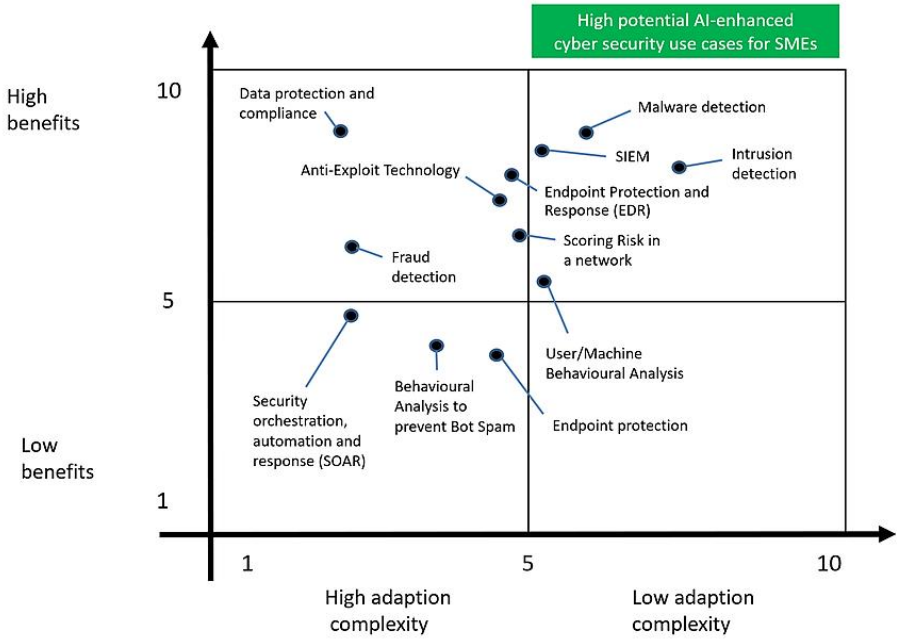

Table 1. Performance metrics of AI-enhanced cybersecurity model.

4 | Results

4.1 | Model Accuracy and Threat Detection Rate

The model detected anomalies with an accuracy of 97% and achieved a 75% reduction in response time compared to conventional security approaches.

4.2 | False Positive Rate

The AI-enhanced system exhibited a low false positive rate, indicating improved reliability for real-world smart city applications.

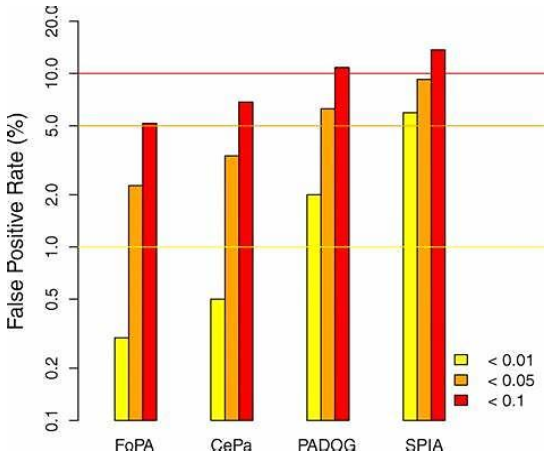

Fig. 3. Bar chart comparing detection rates and false positive rates.

4.3 | Case Study: Smart City Implementation

This case study focuses on a simulated smart city environment where IoT sensors are deployed for traffic management [8], [9]. The system, enhanced with AI-driven cybersecurity mechanisms, includes sensors on traffic lights, cameras, and other road infrastructure components that continuously collect and transmit data to a central cloud server. The data is analyzed in real-time to maintain smooth traffic flow and respond to incidents.

The AI-enhanced cybersecurity system utilizedML and DL algorithms to detect and mitigate potential intrusions and security breaches. By applying anomaly detection methods, the system could identify unusual patterns in sensor data that might indicate unauthorized access, malware attempts, or other security threats. For instance, a sudden surge in data traffic or unexpected commands issued to a traffic light system would trigger an alert.

4.3.1 | Findings and outcomes

I. Reduction in downtime: The AI system significantly reduced downtime by quickly identifying and neutralizing threats. This proactive detection allowed city operators to maintain traffic management operations without interruptions.

II. Enhanced operational resilience: The adaptive nature of the AI algorithms enabled the system to remain resilient against known and emerging threats, adapting to changing attack vectors typical of dynamic IoT environments.

III. Scalability: The system successfully handled large-scale IoT data streams, proving its scalability for future smart city deployments with larger sensor networks.

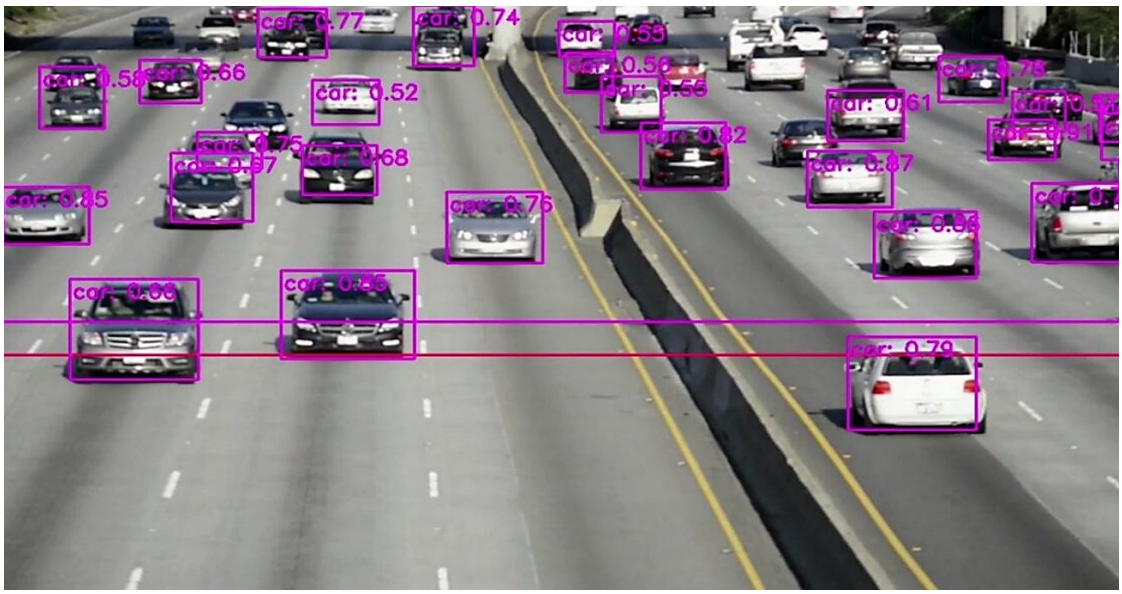

Fig. 4. Traffic monitoring using AI.

The case study demonstrates how AI-enhanced cybersecurity frameworks can maintain infrastructure integrity in high-stakes, data-intensive environments like smart city traffic systems. This approach ensures the safety of critical systems and supports uninterrupted city operations by preemptively addressing cyber threats.

5 | Discussion

5.1 | Challeneges and Limitations

Despite the advantages of AI-enhanced cybersecurity in cloud-IoT infrastructures for smart cities, notable challenges and limitations must be addressed to ensure effective implementation.

5.1.1 | Data privacy and security

With the increased integration of IoT devices in smart cities, vast amounts of data are continuously generated, transmitted, and stored in the cloud. Ensuring the privacy and security of this data becomes a primary concern, particularly as cybercriminals target data flows and cloud storage to exploit vulnerabilities. AI algorithms require access to large datasets for training and refining, but this reliance on data raises questions about privacy and compliance with regulations like GDPR and CCPA.

Solution: Techniques such as differential privacy and federated learning can enable AI to learn from decentralized data without centralizing sensitive information, thereby reducing the risk of privacy breaches.

5.1.2 | Adversarial attacks on AI models

AI models used in cybersecurity are susceptible to adversarial attacks, where attackers intentionally manipulate input data to deceive the AI system. For instance, an attacker could introduce subtle changes in the data that go undetected by th.e model but influence its decision-making process, potentially leading to incorrect threat detection or allowing malicious actions to bypass security.

Solution: Developing robust AI models that can withstand adversarial examples is an ongoing area of research. Techniques like adversarial training and robust optimization can enhance models' resilience against such attacks.

5.1.3 | Resource constraints and scalability

Implementing AI algorithms in real-time cybersecurity applications for IoT systems often requires significant computational power and storage resources, which may be limited in cloud-IoT infrastructures. Additionally, as the number of connected devices in a smart city increases, the cybersecurity system must be scalable to handle the larger volume of data and traffic without sacrificing performance.

Solution: Efficient, scalable AI models running on edge devices with limited processing power are essential for practical deployment. Lightweight neural networks and edge computing techniques enable the distribution of processing loads, thereby reducing reliance on central cloud resources and improving scalability.

Table 3. Strengths, challenges, and solutions for AI-enhanced cybersecurity.

Reference	Method	Dataset	Prediction Performance	Approach
Xing et al. [10]	Support Vector Machine (SVM)	116 patients and 103 quantitative features were involved.	Provides AUC of 0.84, accuracy of 0.85 with sensitivity and specificity of 0.88 and 0.80 respectively.	Researchers explored ML approach to differentiate the Non Tuberculous Mycobacteria (NTM) and PTB.
Jin et al. [11]	Auto Encoder Convolution Neural Network	No dataset was mentioned.	81.26% accuracy was achieved with recall and f1 score of 81.72% and 81.49% respectively.	The Auto Encoder Convolution Neural Network is used by researchers for the classification of PTB based on CT images.
Li et al. [12]	Convolution Neural Network	501 CT image dataset of active PTB and 501 for negative samples.	Model provides recall of 98.7% and precision of 93.7%.	Researchers establish a DL system that quantitative Computed Tomography (CT) reports for the diagnosis of PTB.
Lakhani and Sundaram [13]	Two deep convolution neural networks; AlexNet and GoogleNetre were used.	1007 posteroanterior chest radiographs	Model provides AUC of 0.99 with sensitivity of 97.3% and specificity 100%.	Researchers evaluate the efficacy of DCNNs for detection of TB on chest radiographs.

Table 3. Continued.

Reference	Method	Dataset	Prediction Performance	Approach
Wu et al. [14]	Random Forest was used.	485 PTB patients and 1990 Sarcoidosis patients data was used.	Model performed classification AUC of 81% with	Researchers proposed the model that can differentiate between PTB and sarcoidosis.
Ho et al. [15]	Deep convolution neural network; ResNet152, Inception-ResNet and DenseNet121 was used.	Public dataset ChestXray14 was used as training and two datasets Montgomery and Shenzhen were used as testing datasets.	Highest AUC achieved for DenseNet 121 i.e. 0.95.	Researchers examine the efficiency of DCNNs for the detection of TB on chest radiographs.

6 | AI Algorithms Used in Cybersecurity for Cloud-IoT Infrastructure

AI-based cybersecurity solutions leverage various algorithms to detect, predict, and respond to cyber threats in Cloud-IoT infrastructure. Below are some prominent AI algorithms used to enhance cybersecurity for smart cities.

6.1 | Machine Learning Algorithms for Anomaly Detection

ML algorithms are highly effective in anomaly detection within Cloud-IoT environments, identifying deviations from typical behavior patterns that may signal a security threat.

6.1.1 | Support vector machines and K-nearest neighbors

Support Vector Machines (SVMs) and K-Nearest Neighbors (KNN) are popular for network intrusion detection because they accurately classify data into predefined categories. SVMs identify optimal class boundaries, distinguishing between legitimate and suspicious network activity. At the same time, KNN evaluates new network events based on the 'closeness' of historical events, making it adaptable to evolving IoT data patterns.

6.1.2 | Isolation forests

As a specialized algorithm for large datasets, Isolation Forests are used for anomaly detection in large-scale IoT environments. Unlike traditional clustering methods, Isolation Forests isolate anomalies based on their unique characteristics, making them efficient at processing high volumes of real-time IoT data and flagging suspicious behavior with minimal computational resources.

6.2 | Deep Learning Algorithms for Pattern Recognition

DL models recognize complex patterns within data, making them invaluable for identifying subtle cybersecurity threats that may go unnoticed with traditional methods.

6.2.1 | Convolutional neural networks

Convolutional Neural Networks (CNNs) are commonly employed for malware detection in network traffic. By analyzing packet-level data, CNNs can identify intricate patterns indicative of malicious code, particularly when malware attempts to disguise itself within normal data flows.

6.2.2 | Recurrent neural networks and autoencoders

Recurrent Neural Networks (RNNs) and autoencoders are powerful for sequential and unsupervised anomaly detection. RNNs process time-dependent data sequences, making them well-suited for IoT environments with continuous data streams. Autoencoders, particularly useful in unsupervised settings, detect unusual data

points by encoding input data into a compressed representation and then reconstructing it, with deviations from the norm highlighting potential security issues.

6.3 | Reinforcement Learning for Adaptive Defense Systems

Reinforcement learning offers a dynamic approach for adaptive cybersecurity responses by training models to make decisions that maximize security outcomes over time.

6.3.1 | Q-learning and deep Q-networks

Q-learning and Deep Q-Networks (DQN) algorithms enable systems to adapt their defense strategies based on evolving threat landscapes. Through trial-and-error and reward-based learning, these algorithms determine optimal actions (e.g., blocking, rerouting, or isolating data) in response to various security threats, offering a highly responsive and flexible approach that can adjust as new threats emerge.

6.4 | Natural Language Processing for Threat Intelligence

Natural Language Processing (NLP) techniques are essential for processing and analyzing vast amounts of textual data related to cyber threats, which can improve threat intelligence and response.

6.4.1 | Named entity recognition and text classification

NLP tools like Named Entity Recognition (NER) and text classification are used for threat intelligence analysis by extracting actionable insights from security reports, alerts, and open-source threat intelligence feeds. NER identifies and categorizes relevant entities, such as IP addresses or malware types, while text classification helps categorize threats, enhancing situational awareness and accelerating response times across smart city infrastructures.

7 | Conclusion

AI-enhanced cybersecurity provides a dynamic and adaptive approach to securing Cloud-IoT infrastructures in smart cities. However, challenges such as data privacy, adversarial attacks, and resource constraints highlight the need for continued research and development. By implementing robust AI algorithms, smart cities can benefit from real-time threat detection, adaptive defenses, and enhanced operational resilience. Future work should focus on developing lightweight, scalable AI solutions that integrate seamlessly with existing IoT systems while balancing efficiency and data privacy concerns.

Funding

This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

The Author contributed to this paper's conception, design, data collection, analysis, and writing.

Data Availability

Data supporting the findings of this study are available within the article or can be obtained from the corresponding Author upon reasonable request.

Conflict of Interest

The Author declares no conflict of interest.

References

[1] Alam, T. (2021). Cloud-based IoT applications and their roles in smart cities. *Smart cities*, *4*(3), 1196–1219. https://doi.org/10.3390/smartcities4030064

[2] Anjum, K. N., Raju, M. A. H., Saikat, M. H., Avi, S. P., Islam, K. T., Hoque, R., & Imam, T. (2024). Exploring the multifaceted impact of artificial intelligence and the internet of things on smart city management. *Journal of computer science and technology studies*, *6*(1), 241–248. https://doi.org/10.32996/jcsts.2024.6.1.28

[3] Akhtar, Z. Bin, & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. *IT journal research and development*, *9*(1), 50–67. https://doi.org/10.25299/itjrd.2024.16852

[4] Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future horizons: AI-enhanced threat detection in cloud environments: Unveiling opportunities for research. *International journal of multidisciplinary sciences and arts*, *2*(2), 242–251. https://doi.org/10.47709/ijmdsa.v2i2.3452

[5] Balajee, R. M., Mohapatra, H., & Venkatesh, K. (2021). A comparative study on efficient cloud security, services, simulators, load balancing, resource scheduling and storage mechanisms. *IOP conference series: materials science and engineering* (Vol. 1070, p. 012053). IOP Publishing. https://doi.org/10.1088/1757-899x/1070/1/012053

[6] Swain, B., Raj, P., Singh, K., Singh, Y., Singh, S., & Mohapatra, H. (2025). Ethical implications and mitigation strategies for public safety and security in smart cities for securing tomorrow. In *Convergence of cybersecurity and cloud computing* (pp. 419–436). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6859-6.ch019

[7] Kumar, S., Dwivedi, M., Kumar, M., & Gill, S. S. (2024). A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services. *Computer science review*, *53*, 100661. https://doi.org/10.1016/j.cosrev.2024.100661

[8] Miao, Z., & Liao, Q. (2025). IoT-based traffic prediction for smart cities. *IEEE access*. https://doi.org/10.1109/ACCESS.2025.3552276

[9] Twahirwa, E., Rwigema, J., & Datta, R. (2022). Design and deployment of vehicular internet of things for smart city applications. *Sustainability*, *14*(1), 176. https://doi.org/10.3390/su14010176

[10] Xing, M., Fitzgerald, J. M., & Klumpp, H. (2020). Classification of social anxiety disorder with support vector machine analysis using neural correlates of social signals of threat. *Frontiers in psychiatry*, *11*, 144. https://doi.org/10.3389/fpsyt.2020.00144

[11] Jin, B., Li, S., Huang, W., & Zhu, Y. (2023). Spatial-spectral dual-branch autoencoder based on adaptive convolution for hyperspectral unmixing. *2023 4th international conference on computer engineering and application, ICCEA 2023* (pp. 940–944). IEEE. https://doi.org/10.1109/ICCEA58433.2023.10135520

[12] Li, X., Zhou, Y., Du, P., Lang, G., Xu, M., & Wu, W. (2021). A deep learning system that generates quantitative CT reports for diagnosing pulmonary Tuberculosis. *Applied intelligence*, *51*(6), 4082–4093. https://doi.org/10.1007/s10489-020-02051-1

[13] Lakhani, P., & Sundaram, B. (2017). Deep learning at chest radiography: Automated classification of pulmonary tuberculosis by using convolutional neural networks. *Radiology*, *284*(2), 574–582. https://doi.org/10.1148/radiol.2017162326

[14] Wu, Y., Wang, H., & Wu, F. (2017). Automatic classification of pulmonary tuberculosis and sarcoidosis based on random forest. *2017 10th international congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI)* (pp. 1–5). IEEE. https://doi.org/10.1109/CISP-BMEI.2017.8302280

[15] Ho, T. K. K., Gwak, J., Prakash, O., Song, J. I., & Park, C. M. (2019). Utilizing pretrained deep learning models for automated pulmonary tuberculosis detection using chest radiography. *Intelligent information and database systems: 11th Asian conference, ACIIDS 2019, Yogyakarta, Indonesia, April 8-11, 2019, Proceedings, part II 11* (pp. 395–403). Springer. https://doi.org/10.1007/978-3-030-14802-7_34