A COMPARATIVE STUDY OF AI TOOLS FOR REAL-TIME NETWORK ANOMALY DETECTION AND RESOLUTION

P. SRI LATHA
Research scholar, Department Computer Science & Engineering University of Technology,
Vatika, Jaipur, E-mail:
srilathauot@gmail.com

Prof SUNEEL PAPPALA
Department of Computer Science & Engineering, University of Technology,
Vatika, Jaipur, E-mail:
suneelpappala@gmail.com

ABSTRACT

This study presents a comprehensive overview of existing methods for anomaly detection in IoT networks using machine learning (ML). A detailed analysis of various ML algorithms, both supervised (e.g., Random Forest, Gradient Boosting, SVM) and unsupervised (e.g., Isolation Forest, Autoencoder), was conducted. One of the key elements of IoT systems is effective anomaly detection, which identifies abnormal behavior in devices or entire systems. The performance of the selected algorithms was evaluated using commonly used metrics. The complexity of cyber-attacks makes it difficult to develop efficient tools to detect them. Signature-based intrusion detection has been the common method used for detecting attacks and providing security. However, with the emergence of Artificial Intelligence (AI), particularly Machine Learning, Deep Learning and ensemble learning, promising results have been shown in detecting attacks more efficiently. Telecommunication networks are becoming increasingly dynamic and complex due to the massive amounts of data they process. Traditional methods of anomaly detection, which rely on rule-based systems, are no longer effective in today's fast-evolving telecom landscape. Thus, making AI useful in addressing these shortcomings. This study critically examines the role of Artificial Intelligence (AI), particularly deep learning, in modern anomaly detection systems for telecom networks. Additionally, emerging AI technologies such as Generative Adversarial Networks (GANs) and Reinforcement Learning (RL) are highlighted for their potential to enhance anomaly detection.

Keywords: *Artificial Intelligence (AI), anomaly detection systems, AI technologies, cyber-attacks, Generative Adversarial Networks (GANs).*

INTRODUCTION

A comparative analysis of IoT anomaly detection methods evaluates the strengths and weaknesses of the different approaches, focusing on their applications in different IoT environments. Traditional methods, such as rule-based systems, are simple and easy to interpret, but struggle to cope with the complexity and scale of modern IoT data. In contrast, ML techniques such as decision trees, neural networks, and Support Vector Machines offer greater accuracy and adaptability in detecting subtle and evolving anomalies. Hybrid methods that combine rule-based systems with ML strike a balance between interpretability and efficiency. Unsupervised learning models are particularly useful when tagged data are sparse, but their effectiveness depends heavily on the quality of data preprocessing. Ensemble methods, which combine the results of multiple models, generally improve detection performance by reducing the occurrence of false alarms. Deep learning methods, while efficient, require large datasets and can be computationally expensive, making them less suitable for IoT devices with limited resources. Explainable artificial intelligence (XAI) is becoming increasingly important in anomaly detection to provide transparency and confidence in decisions made by complex models. Real-time detection is crucial for IoT networks, and methods supporting low-latency processing are favored in dynamic

environments. Overall, our benchmarking study highlighted the trade-offs between accuracy, interpretability, computational efficiency, and scalability when choosing the right anomaly detection technique for IoT networks. Traditional security mechanisms, which rely on predefined signatures or static rules, are proving increasingly inadequate in the ever-changing landscape of the IoT. IoT environments are dynamic, with devices constantly interacting, evolving, and generating vast quantities of data, making static security measures inadequate. Anomaly detection, which identifies deviations from the normal behavior of a device or system, is becoming a critical component of modern security strategies. By monitoring patterns and identifying anomalies, anomaly detection can help detect potential threats before they cause damage. Early anomaly detection enables rapid action to prevent data breaches and reduce the likelihood of service disruption. This proactive approach also helps identify and mitigate unauthorized access attempts, strengthening network security. In addition, anomaly detection can adapt to new threats that traditional methods may overlook, providing comprehensive protection. The real-time nature of IoT systems requires security mechanisms that are both flexible and responsive to emerging threats. Implementing robust anomaly detection increases overall system resilience, maintaining both network integrity and operational stability. As IoT ecosystems evolve, modern security systems must evolve to stay ahead of increasingly sophisticated cyber threats.

LITERATURE REVIEW

Izabela Rojek (2024) The growth of the Internet of Things (IoT) and its integration with Industry 4.0 and 5.0 are generating new security challenges. One of the key elements of IoT systems is effective anomaly detection, which identifies abnormal behavior in devices or entire systems. This paper presents a comprehensive overview of existing methods for anomaly detection in IoT networks using machine learning (ML). A detailed analysis of various ML algorithms, both supervised (e.g., Random Forest, Gradient Boosting, SVM) and unsupervised (e.g., Isolation Forest, Autoencoder), was conducted. The performance of the selected algorithms was evaluated using commonly used metrics (Accuracy, Precision, Recall, F1-score). The experimental results showed that the Random Forest and Autoencoder methods are highly effective in detecting anomalies. The article highlights the importance of appropriate data preprocessing to improve detection accuracy. Furthermore, the limitations of a centralized machine learning approach in the context of distributed IoT networks are discussed. The article also presents potential directions for future research in the field of anomaly detection in the IoT.

Sahibzada Saadoon Hammad (2024) Advanced Machine Learning (ML) algorithms can be applied using Edge Computing (EC) to detect anomalies, which is the basis of Artificial Intelligence of Things (AIoT). EC has emerged as a solution for processing and analysing information on IoT devices. This field aims to allow the implementation of Machine/Deep Learning (DL) models on MicroController Units (MCUs). Integrating anomaly detection analysis on Internet of Things (IoT) devices produces clear benefits as it ensures the use of accurate data from the initial stage. However, this process poses a challenge due to the unique

characteristics of IoT. The results of this paper provide a comprehensive overview of anomaly detection using TinyML and MCUs. The main contributions of this survey are the fact that it aims to: (a) study techniques for anomaly detection in ML/DL and validation metrics used in the AIoT; (b) analyse data used in the estimation of models; (c) show how ML is applied in EC using hardware or software; (d) investigate the main microcontrollers, types of power supply, and communication technology; and (e) develop a taxonomy of ML/DL algorithms used to detect anomalies in TinyML. Finally, the benefits and challenges of this kind of TinyML analysis are described.

Li Li (2024) This study presents a comprehensive approach to face detection utilizing the YOLOv8 model, specifically trained on a diverse dataset consisting of images from four individuals. The trained model is seamlessly integrated into an AI module from Huada, a leading AI company, equipped with a camera and LED indicators, enabling real-time face recognition and classification of known and unknown individuals. The model's performance is evaluated across various metrics, demonstrating its high accuracy, robustness, and efficiency in real-world scenarios. Additionally, the deployment process is detailed, showcasing the practical challenges and solutions encountered during the integration into a security application. Our results indicate that YOLOv8 is not only effective in identifying individuals with high precision but also scalable and adaptable to different environments. This work contributes to the development and deployment of advanced face detection systems, with significant implications for security and surveillance applications.

Shahram Latifi (2023) In this research study, various Machine Learning (ML) models are discussed for the purpose of detecting brain anomalies like tumors. In the first step, we review previous work that uses Deep Learning (DL) to classify and detect brain tumors. Next, we present a detailed analysis of the ML methods in tabular form to address the brain tumor morphology, accessible datasets, segmentation, extraction, and classification using DL, and ML models. Finally, we summarize all relevant material for tumor detection, including the merits, limitations and future directions. However, the brain tumor segmentation using ML models suffers from drawbacks due to limited labelled data, variability in tumor appearance, computational memory requirements, transparency in models, and difficulty in integration into clinical workflows. By pursuing techniques such as Data Augmentation, Pre-training, Active-learning, Multimodal fusion, Hardware acceleration, and Clinical integration, researchers and developers can overcome the bottlenecks and enhance the accuracy, efficiency, and clinical utility of ML-based brain tumor segmentation models.

Rakesh Kumar Singh (2023) Recently a lot of medical tablets with special packets in the global market are available. For the safety and purity of the tablet, we need to scan it by developed scanner technology, which should be not more expensive and easily available in the market. The THz technology is one of them. In the proposed work, we have tasted tablet images with the help of the THz super-resolution scanner, which is already available in our lab. The AI machine learning data concept has been investigated. Good resolution of images has been obtained. Furthermore, the challenging research problems are

discussed. Finally, it summarizes the recent updates in terahertz technology for drug inspection and medical applications with potential research challenges.

Semih Aslan (2021) This research presents an improved real-time face recognition system at a low resolution of 15 pixels with pose and emotion and resolution variations. We have designed our datasets named LRD200 and LRD100, which have been used for training and classification. The face detection part uses the Viola-Jones algorithm, and the face recognition part receives the face image from the face detection part to process it using the Local Binary Pattern Histogram (LBPH) algorithm with preprocessing using contrast limited adaptive histogram equalization (CLAHE) and face alignment. The face database in this system can be updated via our custom-built standalone android app and automatic restarting of the training and recognition process with an updated database. Using our proposed algorithm, a real-time face recognition accuracy of 78.40% at 15 px and 98.05% at 45 px have been achieved using the LRD200 database containing 200 images per person. With 100 images per person in the database (LRD100) the achieved accuracies are 60.60% at 15 px and 95% at 45 px respectively. A facial deflection of about 30° on either side from the front face showed an average face recognition precision of 72.25%-81.85%.

Weiping Liu (2020) Due to the wave characteristics of light, diffraction occurs when the light passes through the optical system, so that the resolution of the ordinary far-field optical system is limited by the size of the Airy disk diameter. There are various factors that cause image quality degradation during system detection and imaging, such as optical system aberrations, atmospheric interference, defocusing, system noise and so on. Super-resolution optical imaging technology is the most innovative breakthrough in the optical imaging and detection field in this century. It goes beyond the resolution limit of ordinary optical systems or detectors, and can get more details and information of the structure, providing unprecedented tools for various fields. Compared with ordinary optical systems, super-resolution systems have very high requirements on the signals to be detected, which cannot be met by ordinary detection techniques. Vacuum photoelectric detection and imaging technology is equipped with the characteristics of high sensitivity and fast response. It is widely used in super-resolution systems and has played a great role in super-resolution systems.

Frank J. Louws (2019) Anthracnose of strawberry, caused primarily by the fungal pathogens belonging to Colletotrichum acutatum species complex (CASC) and C. gloeosporioides species complex (CGSC) is an economically important disease in the Southeast United States. Quiescently infected (QI) planting stock is one of the most important sources of inoculum in the fruiting field that can only be reliably detected by highly sensitive real time quantitative PCR (q-PCR) assay. In this study, a q-PCR assay was developed and optimized that can discriminate anthracnose fruit rot (AFR) and anthracnose crown rot (ACR) causing species based on the difference in post PCR melting temperatures of amplicons. Controlled environment grown plants artificially inoculated with different levels of CASC and CGSC showed a significant ($P < 0.001$) correlation with levels of quantification expressed by Ct values in q-PCR from petioles and leaf blades. The leaf

blade was a significantly larger reservoir of QI than that of the petiole. Both TaqMan and SYBR Green assay showed similar sensitivity and specificity. Detection of QI on leaves at young middle and older stages from inoculation with same number of conidia indicated that middle aged leaves were the best for assessing QI.

Calum MacAulay (2017) Cervical cancer remains a critically important problem for women, especially those women in the developing world where the case-fatality rate is high. There are an estimated 528,000 cases and 266,000 deaths worldwide. Established screening and detection programs in the developed world have lowered the mortality from 40/100,000 to 2/100,000 over the last 60 years. The standard of care has been and continues to be: a screening Papanicolaou smear with or without Human Papilloma Virus (HPV) testing; followed by colposcopy and biopsies and if the smear is abnormal; and followed by treatment if the biopsies show high grade disease (cervical intraepithelial neoplasia (CIN) grades 2 and 3 and Carcinoma-in-situ). Low grade lesions (Pap smears with Atypical Cells of Uncertain Significance (ASCUS), Low Grade Squamous Intraepithelial Lesions (LGSIL), biopsies showing HPV changes or showing CIN 1); are usually followed for two years and then treated if persistent. Treatment can be performed with loop excision, LASER, or cryotherapy. Loop excision yields a specimen which can be reviewed to establish the diagnosis more accurately. LASER vaporizes the lesion and cryotherapy leads to tissue destruction.

Harry Wechsler (2015) Despite extensive research, timing channels (TCs) are still known as a principal category of threats that aim to leak and transmit information by perturbing the timing or ordering of events. Existing TC detection approaches use either signature-based approaches to detect known TCs or anomaly-based approach by modeling the legitimate network traffic in order to detect unknown TCs. Unfortunately, in a software-defined networking (SDN) environment, most existing TC detection approaches would fail due to factors such as volatile network traffic, imprecise timekeeping mechanisms, and dynamic network topology. Furthermore, stealthy TCs can be designed to mimic the legitimate traffic pattern and thus evade anomalous TC detection. In this paper, we overcome the above challenges by presenting a novel framework that harnesses the advantages of elastic resources in the cloud. In particular, our framework dynamically configures SDN to enable/disable differential analysis against outbound network flows of different virtual machines (VMs).

Understanding AI Anomaly Detection

Definition and Principles of AI Anomaly Detection

AI anomaly detection refers to the process of identifying patterns or behaviors in data that deviate from expected or normal activity. These unexpected data points are flagged as anomalies or outliers, which may indicate a potential issue or event that warrants further investigation. AI-based anomaly detection systems leverage advanced technologies like machine learning (ML) and deep learning (DL) to learn from historical data and automatically recognize normal behavior. Once trained, the system can spot deviations in real-time and alert stakeholders about potential issues. The core principle behind AI anomaly detection is its ability to automate the identification process, allowing for rapid and accurate analysis of vast datasets. Through training the anomaly detection

model on historical data, normal patterns of behavior are established, enabling the system to become proficient at detecting subtle inconsistencies or deviations that may signal a problem. This continuous learning process enables AI systems to evolve and adapt to new conditions and dynamic environments.

How Does AI Anomaly Detection systems Work?

AI anomaly detection involves advanced machine learning algorithms that analyse and identify unusual patterns in data, systems, or behaviors. AI anomaly detection systems continuously learn from incoming data to distinguish between normal and abnormal patterns. This allows them to identify anomalies that could indicate underlying issues, such as equipment malfunctions, security threats, or system inefficiencies.

AI Anomaly Detection Process

Data Collection and Preprocessing

The first step in anomaly detection is gathering data from various sources like video data, production lines, industrial cameras, or IoT devices. This data often requires cleaning, normalizing, and segmenting to ensure it's in the right format for the anomaly detection models. Preprocessing helps remove noise, handle missing values, and standardize the data for effective processing.

Sensor Integration and Perception

Once the data is prepared, feature selection is essential. It involves identifying the most relevant attributes that help the AI model distinguish between normal and abnormal patterns. In manufacturing, these features could include temperature, pressure, or vibration levels. Selecting the right features is crucial for ensuring the model focuses on the most impactful data points for anomaly detection.

Robustness and Scalability

After data preparation and feature selection, the AI model is trained using historical data. The model learns what constitutes normal behavior, using machine learning techniques like supervised or unsupervised learning. In supervised learning, labeled data with examples of normal and abnormal conditions is used, while unsupervised learning detects outliers without predefined labels.

Anomaly Detection

Once trained, the model analyzes new data in real time, identifying anomalies by comparing incoming data against learned patterns. These anomalies can be outliers, context-specific deviations, or unusual patterns over time. The system flags anomalies for further investigation or immediate action, improving its detection capabilities over time.

Video Anomaly Detection vs. Other Anomaly Detection Methods

Video anomaly detection offers significant advantages over traditional methods, especially in complex, dynamic environments where visual context is crucial. Unlike traditional systems that analyze structured data like sensor readings or logs, video anomaly detection uses visual data captured by cameras, allowing the system to understand and interpret actions and events. This enables real-time detection of anomalies such as unauthorized access, abnormal behavior, or equipment malfunctions.

Vision-based anomaly detection can track movements, identify behavioral changes, and detect subtle discrepancies that traditional methods may miss, making it ideal for security surveillance, industrial environments, and retail spaces. In contrast, traditional anomaly detection systems rely on predefined thresholds and statistical

models to flag numerical deviations, often struggling to capture the complexity of dynamic environments. For example, a sensor may detect an abnormal temperature but can't determine whether it's due to an operational change or failure. Additionally, automated anomaly detection with video can identify previously unseen anomalies by learning from new patterns, offering a more adaptive, comprehensive solution. While traditional systems excel in numerical monitoring, visual anomaly detection enhances situational awareness and accuracy, providing a more dynamic and context-rich approach.

The Advantages of Anomaly Detection Software

Anomaly detection software enhances anomaly detection capabilities by identifying potential issues or irregularities before they escalate into larger, costly problems. It continuously analyzes real-time data, detecting even the smallest deviations from normal patterns. Early detection of anomalies mitigates risks, improves efficiency, and reduces the impact of potential failures. Video anomaly detection software can also monitor visual data to identify irregularities in real-time.

Reduced Downtime

One major benefit of automated anomaly detection platform is its ability to reduce unplanned downtime. By predicting machines failures, it enables proactive maintenance. This minimizes costly breakdowns, ensuring continuous production and operational efficiency in sectors like manufacturing, healthcare, and energy. Automated anomaly detection maximize uptime, resource utilization, and the overall performance of critical systems. Visual monitoring in dynamic environments further contributes to minimizing operational disruptions.

Improved Accuracy

AI anomaly detection platform uses advanced machine learning algorithms to analyse large datasets with precision. It detects subtle deviations from expected behavior that might go unnoticed otherwise, reducing false positives and improving decision-making. This enhances overall system reliability and reduces risks. Automated anomaly detection continuously processes data, offering more accurate results than traditional systems and making it invaluable for real-time applications.

Enhanced Decision-Making

By providing timely and accurate insights into system performance, anomaly detection software enhances decision-making. It supports businesses in optimizing production schedules, improving equipment maintenance, and preventing fraud. With early anomaly detection, businesses can address issues before they escalate, ensuring predictive analytics for effective strategies and better resource allocation. Vision-based anomaly detection also contributes by offering data analysis that enable more informed decisions, enhancing operational outcomes and improving overall productivity.

Cost Savings

Early anomaly detection leads to substantial cost savings by identifying potential issues before they escalate into costly repairs, system failures, or financial losses. By detecting irregularities at an early stage, businesses mitigate risks, improve resource allocation, and avoid unplanned downtime. Automated detection of anomalies further reduces operational costs by eliminating the need for manual oversight and intervention, optimizing operational efficiency. These capabilities ensure long-term financial stability by enhancing productivity,

minimizing the impact of anomalies, and improving overall system reliability.

CONCLUSION

AI platforms for anomaly detection are transforming industries by improving operational efficiency, minimizing risks, and enhancing overall quality. In manufacturing, the combination of AI, computer vision, and IoT allows businesses to monitor processes in real-time, predict equipment failures, and ensure product consistency. By identifying potential issues early, these systems enable proactive maintenance, reduce downtime, and optimize production workflows. After outlining the limitations of traditional rule-based monitoring approaches, various supervised and unsupervised machine learning algorithms were explored for developing robust anomaly detection models tailored to network environments. Specifically, clustering, isolation forest, auto encoders and RNN models were identified as commonly used techniques. To demonstrate integration of the ML models with existing monitoring tools, an architecture was proposed to add AI modules as plug-ins. Further testing methodology and sample results validated the AI approach can significantly reduce false positives while enhancing speed and accuracy of anomaly identification. While the potential of AI-driven monitoring was exhibited, challenges around acquiring sufficient representative training data, feature engineering expertise, and balancing model changes were also discussed.

REFERENCES

1. *Izabela Rojek (2024), "A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study", Appl. Sci., ISSN:2076-3417, vol. 14(24), https:// doi.org/10.3390/app142411545*
2. *Sahibzada Saadoon Hammad (2024), "Anomaly detection based on Artificial Intelligence of Things: A Systematic Literature Mapping", Internet of Things, issn: 2327-4662, vol. 25, https://doi.org/10.1016/j.iot.2024.101063*
3. *Harry Wechsler (2015), "Real-Time Timing Channel Detection in a Software-Defined Networking Virtual Environment", Intelligent Information Management, issn:2160-5920, vol.7, pages.283-302.*
4. *Calum MacAulay (2017), "Established and Emerging Optical Technologies for the Real-Time Detection of Cervical Neoplasia: A Review", Journal of Cancer Therapy, issn:2151-1942, vol. 8, pages. 1241-1278.*
5. *Semih Aslan (2021), "An Improved Real-Time Face Recognition System at Low Resolution Based on Local Binary Pattern Histogram Algorithm and CLAHE", Optics and Photonics Journal, issn: 2160-889X, vol. 11, pages. 63-78.*
6. *Shahram Latifi (2023), "A Survey of Techniques for Brain Anomaly Detection and Segmentation Using Machine Learning, International Journal of Communications, Network and System Sciences, issn: 1913-3723, vol. 16, pages. 151-167.*
7. *Frank J. Louws (2019), "Simultaneous Detection of Colletotrichum acutatum and C. gloeosporioides from Quiescently Infected Strawberry Foliage by Real-Time PCR Based on High Resolution Melt Curve Analysis", American Journal of Plant Sciences, issn:2158-2750, vol.10, pages.382-401.*
8. *Li Li (2024), "Advanced Face Detection with YOLOv8: Implementation and Integration into AI Modules", Open Access Library Journal, issn:2333-9721, vol. 11, pages. 1-18.*
9. *Rakesh Kumar Singh (2023), "Investigation of Tablet Defects by AI Based Terahertz Technology", Open Journal of Antennas and Propagation, issn: 2329-8413, vol. 11, pages. 26-35.*
10. *Weiping Liu (2020), "Application of Vacuum Photoelectric Detection Technology in Super-Resolution System", Optics and Photonics Journal, issn: 2160-889X, vol. 10, pages. 141-148.*