AI-Powered Driven Intrusion Systems in Cyber Security and Zero-Day Attack Detection

Hemant Singh Patel[1], Chandra Shekhar Gautam[2], Akhilesh A. Waoo[3]*

[1]Department of Computer Science and Engineering FE&T, AKS University, Satna, MP, India
[2]Department of Computer Science and Engineering FE&T, AKS University, Satna, MP, India
[3]Department of Computer Science and Engineering FE&T, AKS University, Satna, MP, India

---***---

Abstract - AI-powered intrusion systems are becoming essential as cyber threats grow more complex and unpredictable. This review examines how modern artificial intelligence techniques strengthen intrusion detection by learning attack patterns, adapting to new behaviors, and identifying previously unknown vulnerabilities. The paper highlights the role of machine learning, deep learning, and hybrid intelligent models in improving detection accuracy, reducing false alarms, and enhancing real-time analysis. Special attention is given to the challenge of zero-day attacks, where no prior signatures exist; AI-based models address this gap by focusing on anomaly recognition and behavior-driven insights. The review also explores recent developments, comparative performance trends, and practical limitations that influence deployment in real-world networks. Overall, the study underscores how AI-driven intrusion detection systems provide a proactive defense layer capable of evolving with emerging threats and supporting more resilient cybersecurity operations.

Key Words: AI intrusion detection, cybersecurity systems, zero-day attack analysis, intelligent threat monitoring, anomaly detection models, adaptive security frameworks.

1.NTRODUCTION

The New cybersecurity research focuses on using artificial intelligence to overcome the limits of traditional signature-based intrusion detection methods, especially against evasive threats like zero-day attacks. Adding AI to network intrusion detection systems addresses ongoing changes in attack tactics and the growing complexity of enterprise IT infrastructure. Studies consistently show that hybrid approaches that combine machine learning and deep learning algorithms produce better results, adaptive learning, and quick responses, which are crucial for protecting modern infrastructures. These intelligent systems automatically examine complex system activity data and network traffic to spot slight deviations from normal behaviour that may be hard for people to see. Notably, meta-analyses indicate that hybrid models achieve over 96% detection accuracy and lower false positives compared to earlier methods. Current research also defends against adversarial attacks with strong explainable AI systems and emphasises standardised testing protocols to counter dataset bias and adversarial threats. Cost-benefit analyses and field trials in various sectors, such as healthcare and smart cities, highlight the clear advantages of AI-driven intrusion detection systems for both tactical security and strategic planning. Ongoing work aims to develop efficient, ethical, and scalable frameworks that function effectively in diverse, real-time, and limited-resource environments, with a constant focus on zero-day detection and system compatibility.

2.Comprehending Intrusion Detection In The Ai Era

The maturity of intrusion detection systems from static conventional models to AI-based frameworks is a turning point in cybersecurity. With growing sophistication and complexity in cyber threats, human-dependent rule-based detection strategies tend to be ineffective in detecting understated and novel patterns of attacks. Artificial intelligence brings about a fundamental shift by making it possible for systems to independently learn from experience, evolve in response to emerging threat landscapes, and make data-driven decisions in near real time. Underpinning AI-facilitated intrusion detection is the capacity to analyse vast and diverse streams of data from network packets, and system logs through to user behaviour analytics with sophisticated machine learning algorithms. Through the ability to spot complex correlations and distil hidden features, these systems provide a quality of threat detection that outpaces orthodox heuristics. Deep learning architectures,

such as convolutional and recurrent neural networks, further enable detection engines to represent temporal dependencies and sophisticated behaviour sequences characteristic of multi-stage attacks. In addition to pure detection, AI-powered systems help mitigate false positives, a perennial pain point of IDS operations, by optimising anomaly thresholds and contextualising alerts according to historical patterns. The use of explainable AI methods provides a guarantee that notices and automatic responses are transparent and allow human analysts to comprehend the reasoning behind identified threats.

2.1.Fundamental concepts of intrusion detection

At its core, intrusion detection is based on the constant monitoring and analysis of network or system activity to find unauthorised or malicious action. The fundamental concepts that underpin successful intrusion detection systems (IDS) include the capability to tell normal patterns of use from those that could indicate an impending threat, whether through recognised attack signatures or unusual activity outside of defined baselines. Two major detection approaches constitute the foundation of intrusion detection: signature-based detection and anomaly-based detection. Signature-based detection is based on pre-programmed patterns or "signatures" for known threats, searching network traffic or system logs for exact matches.

Although very powerful against attacks previously known to it, this method has difficulty recognising new threats like zero-day exploits that do not yet possess a recognised signature. On the other hand, anomaly-based detection creates a behavioural profile of standard system or network behaviour and alerts on any deviations that could be a sign of an intrusion. This method allows detection of novel or unknown threats but needs to use advanced algorithms to reduce the false positives caused by genuine but out-of-pattern activity.

2.2.Types of intrusion detection systems (signature, anomaly, hybrid)

Intrusion detection systems (IDS) are commonly classified based on their detection methods and deployment models. The basic types, according to detection methods, are signature-based, anomaly-based, and hybrid systems, each with its own strengths and weaknesses in safeguarding networks against malicious behavior.

2.2.1.Signature-Based Intrusion Detection: Signature-based IDS employs a pattern-matching model, matching network traffic and system behavior against a database of established attack signatures or threat fingerprints. Signature-based IDS is particularly effective at detecting previously seen threats with well-known signatures, facilitating the rapid detection of common exploits, such as known malware, worms, and exploit kits. Signature-based systems are unable to detect new or zero-day attacks whose signatures are not yet in the database, limiting their utility in dynamic threat environments.

2.2.2.Anomaly-Based Intrusion Detection: Anomaly detection, on the other hand, creates a baseline model of normal behavioural patterns in an observable system or network. By applying statistical analysis, machine learning, or heuristic models, deviations from this norm such as unusual traffic spikes, unexpected access patterns, or unusual system calls are identified as potential intrusions. This approach is especially useful for identifying zero-day and unknown attacks, but can be plagued by false positives from legitimate but rare behaviour, requiring rigorous tuning and awareness of context.

2.2.3.Hybrid Intrusion Detection: Hybrid IDS marries the methods of signature and anomaly detection to harness the benefits of both. By incorporating known attack signature databases with adaptive models of anomaly detection, hybrid systems offer an improved defence that can recognize known and future threats. Hybrid detection improves the accuracy of detection and minimizes false alarms compared to either method used in isolation. Hybrid IDS frameworks tend to draw from multiple sources of information, such as host-based monitors and network sensors, to create a consolidated threat landscape view.

2.3.Limitations of conventional strategies

Conventional intrusion detection systems, which are mainly focused on signature-based approaches and static rule sets, are severely limited in responding to modern-day cybersecurity threats. Their reliance on established threat signatures makes them of little use against new attack vectors, especially zero-day attacks that materialise without advance signals or known patterns. In turn, such systems tend not to be able to detect quickly mutating, polymorphic malware and advanced adversarial techniques intended to bypass static defences. In addition, conventional IDS will normally produce large numbers of alerts, some of which are false positives due to benign or anomalous yet valid network activity.

Such flooding can harden the security teams, causing delays in response and alert fatigue through desensitization. Manual signature database updating and tuning further place operational loads, constraining the speed and scalability of threat detection. Also, traditional methods are not contextually aware or adaptive learners, limiting the capability to analyze sophisticated multi-stage attacks or nuanced behaviour changes over time. Without the incorporation of real-time analysis and automated response functions, such systems offer reactive, not proactive, security stances.

3.The Art Of Artificial Intelligence For Cyber Defense

Artificial intelligence (AI) has emerged as a critical building block of contemporary cyber defence, significantly revolutionizing the manner in which organisations identify, examine, and counter cyber threats. In contrast to conventional security systems based on static signatures and rules, AI-based systems utilize adaptive learning methodologies that facilitate ongoing development in the wake of a constantly shifting threat environment. At the forefront of AI's capabilities in cyber defence are machine learning algorithms capable of mining vast datasets to uncover hidden patterns and correlations among seemingly disparate events. Supervised learning models leverage historical attack

data to classify malicious behaviours automatically, while unsupervised learning methods excel at identifying novel anomalies suggestive of previously unseen threats. Deep learning, a branch of AI, continues these possibilities through multi-layered neural networks that can represent sophisticated, high-dimensional data with greater precision. This enables subtle identification of sophisticated attack modes like polymorphic malware and multi-stage penetration attempts. Reinforcement learning continues to augment these technologies by allowing systems to dynamically adjust defensive stances based on feedback from changing threat situations.

3.1.Machine Learning Models for Behavioural Analysis

Behavioural analysis in cybersecurity uses machine learning (ML) to create evolving models of typical system or user behaviour, allowing the identification of suspicious deviations that signal cyber attacks. In contrast to static rule-based systems, machine learning systems constantly examine vast and intricate data like users' activities, network flows, and system logs to learn patterns and detect anomalies in real time. Supervised learning models are usually used when labelled sets of benign and malicious behavior are available.

These models, such as decision trees, support vector machines, and neural networks, categorize activities by learning from past data to enable accurate identification of known threat behavior. Their dependence on labelled examples, however, can impair adaptability to unknown or new attacks. Unsupervised learning methods solve this by detecting outliers without being pre-labelled, seeking patterns in on unlabelled data, and raising alarms on deviant activities based deviation from learned norms.

3.2.Deep learning frameworks for real-time detection.

Deep learning frameworks have emerged as powerful tools for real-time cyber threat detection, addressing the limitations of traditional machine learning by their ability to automatically learn hierarchical representations from raw, high-dimensional data.

These frameworks utilise multi-layered neural network architectures such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks to capture spatial and temporal features critical to identifying complex attack patterns. Convolutional neural networks excel in processing structured data, such as network traffic flows and system event sequences,

by detecting localised patterns and anomalies that signal malicious activity. Recurrent neural networks and their variants, like LSTM, are particularly adept at modelling sequential data, enabling the detection of multi-step intrusion attempts and temporal correlations in real-time streams.

3.3.Threat intelligence natural language processing

Natural Language Processing (NLP) significantly enhances threat intelligence in cybersecurity. It makes it possible to automatically comprehend, examine, and draw insights from vast volumes of unstructured text data, such as security reports, social media messages, and dark web communications. NLP methods, including named entity recognition, sentiment analysis, and topic modeling, assist in the discovery of significant indicators of compromise (IOCs), attackers' infrastructures, and developing threats.

This automation accelerates the threat intelligence workflow, reduces human mistakes, and allows security teams to get ahead of emerging cyber threats. By connecting disparate chunks of data and allowing for analysis in multiple languages, NLP gives a complete picture of the threat ecosystem.

It also helps to anticipate attacks through the ability to recognize faint patterns in language that predict possible future threats, which enables proactive cyber defense. Current NLP solutions in cybersecurity allow for quicker detection of threats, improved incident response, and a broader worldwide intelligence view required to address complex and new cyber threats.

4.Architecture Of An Ai-Driven Intrusion Detection System

An AI-based intrusion detection system (IDS) is composed of several interconnected units, which collaborate to observe, identify, and react to cyber attacks with increased intelligence and velocity. The architecture of the system is designed in layers, which play an essential role in the cybersecurity defence system.

4.1.Data Acquisition Layer

This foundation layer emphasizes uninterrupted gathering of varied data essential for threat detection. It aggregates inputs from network traffic, system logs, application events, user activity logs, and endpoint sensors. Diversity and the amount of data offer detailed visibility into the operating environment to facilitate the detection of subtle and intricate attack patterns.

4.2.Data Preparation Layer

Raw data tends to be large and noisy, so it needs intensive cleaning and transformation. This layer cleans and transforms raw data incoming from normalisation, noise filtering, and signal enhancement processes to make it consistent and reliable. It also structures the data in forms appropriate for later analysis.

4.3.Feature Engineering Layer

Critical behavioural characteristics and signs are drawn and built here. Statistical analysis, transformation, and selection identify the most pertinent features, like abnormal packet rates, access irregularities, or sequence anomalies, in the most relevant manner through biomedical research. The detection algorithms' precision and performance are greatly enhanced in this step.

4.4.Detection Engine

Within the core of the architecture, the detection engine utilizes sophisticated models that are able to provide supervised, unsupervised, or hybrid learning. The engine performs ongoing analysis in relation to matching ongoing activity with learned patterns in order to label events as normal or suspicious. The engine adapts dynamically by way of model update mechanisms to improve its ability to detect known and unknown threats.

4.5.Decision and Response Module

Once a threat has been detected, this module triggers corresponding countermeasures. It enables real-time alerting to security analysts, automated containment through IP blocking or session termination, and fine-grained logging to support forensic analysis. The module trades immediacy and accuracy to maximize defensive action while minimizing false alarms.

5.Conquering Zero-Day Attacks Through Predictive Intelligence

Zero-day attacks constitute one of the most daunting challenges in cybersecurity because they exploit as-yet unknown vulnerabilities, rendering conventional signature-based defenses useless. Predictive intelligence provides a proactive approach by foretelling attack vectors before exploitation, thus bridging the gap between vulnerability discovery and response to an incident.

5.1.Nature and Complexity of Zero-Day Vulnerabilities

Zero-day vulnerabilities are not yet announced and fixed by the software developers or vendors, which are security weaknesses. Intruders use such unknown vulnerabilities to breach systems with less notice, frequently utilizing advanced evasion tactics and multi-stage attack routines. The uncertain nature and expansive effect of zero-day exploits necessitate new detection and prevention methods beyond reactive defense strategies.

5.2.Predictive Modelling for Early Warning

Predictive intelligence makes use of sophisticated data modelling and analysis to anticipate probable attack scenarios. By excavating historical attack data, vulnerability announcements, exploit trending, and behavioral indicators, predictive models find early signs of suspicious events that could indicate prep work for zero-day attacks. Machine learning and deep learning allow for ongoing learning from changing threat environments to pick up on faint anomalies before any harm is caused.

5.3.Anomaly Detection and Behavioural Profiling

Effective predictive mechanisms target behavioral anomalies that contrast with known norms throughout network traffic, system calls, and user behavior. Such profiling captures novel attack techniques previously unknown by marking abnormal sequences or patterns indicative of zero-day exploit attempts. Together with context awareness, these signs help to suppress false positives and improve threat prioritization.

6.Embedding Explainable Ai Into Security Systems with Image

Modern security systems increasingly depend on sophisticated computational models for threat detection and response. To foster trust and effective human control, these systems will need to embed mechanisms that render their decisions comprehensible and transparent to security professionals.

6.1.Transparency: Illuminates how alerts and classifications are produced, allowing analysts to validate the correctness of computerized decisions.

6.2.Trust Building: Facilitates trust in system outputs by providing insight into underlying reason processes.

6.3.Accountability: Facilitates regulatory compliance through audit trails and explanations for security actions.

6.4.Error Reduction: Aids in the separation of true threats from false alarms by explaining decision factors.

Table -1: Explainability Integration Elements

Aspect	Description	Examples
Interpretable Models	Simple algorithms are inherently transparent	Decision trees, Rule-based systems
Post-Hoc Analysis	Explanations derived after prediction	SHAP, LIME, Counterfactual analysis

Feature Attribution	Mapping the impact of input features on output	Importance scores, Attention maps
Visualization	Intuitive display supporting human understanding	Graphs, Heatmaps, Flowcharts

7.Comparative Analysis Of Ai Algorithms In Intrusion Detection

Choosing the right computational method to use in intrusion detection is essential for optimal performance, accuracy, and operational efficacy. Different algorithms have inherent strengths and weaknesses along various dimensions, including accuracy of detection, false positives, computational requirements, and adaptability. A comparative analysis of the most widely used intelligent algorithms used in intrusion detection systems follows below.

- **Key Algorithms Examined**

Decision Trees- Tree-like hierarchical models for classifying behaviour through feature splits. They are known for interpretability and efficiency, but can overfit noisy data. Support Vector Machines (SVM)- Good in high-dimensional spaces; can generate optimal decision boundaries. SVMs are sensitive to parameter settings and can be poor with extremely large sets of data.

7.1.K-Nearest Neighbours (KNN): A light, instance-based technique for classification based on closeness to training samples. Effective for smaller data sets, but computationally heavy when the volume of data increases.

7.2.Artificial Neural Networks (ANN): Approximate intricate nonlinear relationships through interlinked computational nodes. Ductile and robust, but they need large training data and lack interpretability.

7.3.Deep Learning Models (CNN, RNN): Sophisticated architectures with the ability to automate feature extraction and recognition of temporal patterns, performing well on intricate datasets. Computationally intensive but provides high accuracy.

7.4.Random Forests: An Ensemble technique of using several decision trees together to enhance generalisation, avoiding overfitting, and increasing robustness.

7.5.Anomaly Detection Models: Unsupervised methods that aim at discovering departures from regular behavior; critical for unknown threat detection but vulnerable to false positives.

Table -2: Performance Evaluation Metrics

Algorithm	**Accuracy**	**False Positive Rate**	**Computational Cost**	**Adaptability**	**Interpretability**
Decision Trees	Moderate	Moderate	Low	Moderate	High
SVM	High	Low	Moderate	Moderate	Low
KNN	Moderate	Moderate	High	Low	Moderate
ANN	High	Moderate	High	High	Low
Deep Learning	Very High	Low	Very High	Very High	Low
Random Forest	High	Low	Moderate	High	Moderate
Anomaly Detection	Variable	High	Moderate	High	Moderate

8. CONCLUSIONS

AI-powered intrusion detection systems represent a transformative advancement in cybersecurity, offering capabilities that extend far beyond the limitations of traditional rule-based and signature-driven approaches. As cyber threats grow more sophisticated, dynamic, and evasive, particularly in the form of zero-day attacks, intelligent detection models provide the adaptability and analytical depth required for effective defence. Through machine learning, deep learning, behavioural modelling, and predictive intelligence, these systems continuously learn from evolving threat landscapes and identify anomalies that would otherwise remain unnoticed. Their ability to process large-scale network data in real time enables proactive detection, faster response, and reduced false alarms, ultimately strengthening the resilience of mode

The insights and comparative analyses presented in this study demonstrate that hybrid AI frameworks, explainable decision models, and predictive mechanisms significantly enhance accuracy and operational reliability in intrusion detection. Continued research collaboration and access to high-quality academic resources remain essential for further innovation. In this context, the availability of related publications through platforms such as LNCS Online supports ongoing progress. Subscribers to the Lecture Notes in Computer Science series can access full papers, while non-subscribers are limited to abstracts and may request complete versions as needed. Overall, AI-driven.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all the individuals and institutions who supported the development of this research on AI-powered driven intrusion systems and zero-day attack detection in cybersecurity. I am deeply thankful to my academic mentors for their guidance, thoughtful feedback, and continuous encouragement, which greatly strengthened the quality and direction of this study. Their expert advice helped me understand complex concepts related to artificial intelligence, anomaly detection, and modern security frameworks.

I also extend my appreciation to the faculty members and colleagues who shared valuable suggestions during discussions and provided insights that enhanced the clarity of the analysis. Their perspectives contributed significantly to refining the structure and presentation of the research content. I am grateful to the research communities, digital libraries, and technical repositories whose resources offered access to high-quality literature, datasets, and benchmark studies that were essential for reviewing AI-based intrusion detection methods.

My heartfelt thanks go to the innovators and researchers whose work in cybersecurity and intelligent threat detection laid the foundation for understanding the evolving landscape of zero-day attacks. Lastly, I acknowledge the constant support of my family and friends, whose motivation and encouragement helped me stay focused throughout this research journey

REFERENCES

1. Clustering of Big Data Using Genetic Algorithm in Hadoop MapReduce Chandra AI-Powered Shekhar Gautam1 and Mr. L N Soni 2 Dr. Prabhat Pandey3 European Chemical Bulletin Volume 11, Year 2023.

2. Hashim, K. A., Yussoff, Y. B. M., & Shahbudin, S. B. (2025). Mitigating Zero-Day Vulnerabilities in IIoT Systems: Challenges and Advances in AI-Powered Intrusion Detection Systems. Mesopotamian Journal of CyberSecurity, 5(3), 1184-1198.

3. Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI AI-based intrusion detection system. Measurement: Sensors, 28, 100827.

4. Johnson, A. (2024). Leveraging AI for zero-day attack detection: challenges and future directions. Journal of Artificial Intelligence Research, 4(2), 123-128.

5. Guo, Y. (2023). A review of machine learning-based zero-day attack detection: Challenges and future directions. Computer communications, 198, 175-185.

6. Raja, M. S. R. S. (2025). The Rise of AI-Driven Network Intrusion Detection Systems: Innovations, Challenges, and Future Directions. International Journal of AI, BigData, Computational and Management Studies, 1(1), 1-10.

7. Rai, H. M., Pal, A., Ergash o'g'li, R. A., Ugli, B. A. K., & Shokirovich, Y. S. (2025). Advanced AI-Powered Intrusion Detection Systems in Cybersecurity Protocols for Network Protection. Procedia Computer Science, 259, 140-149.

8. Niogi, D., Kumar, D. D., Ranjan, D., & Singh, J. (2023, May). Recent Advances and Future Directions in AI-Based Intrusion Detection Systems for Network Security. In Proceedings of the KILBY 100 7th International Conference on Computing Sciences.

9. Alzaylaee, M. K. (2025). Enhancing Cybersecurity Through Artificial Intelligence: A Novel Approach to Intrusion Detection. International Journal of Advanced Computer Science & Applications, 16(4).

10. Mohale, V. Z., & Obagbuwa, I. C. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: enhancing transparency and interpretability. Frontiers in Computer Science, 7, 1520741.

11. Sayduzzaman, M., Rahman, A., Tamanna, J. T., Kundu, D., & Rahman, T. (2024). Interoperability and an explicable AI-based zero-day attacks detection process in a smart community. arXiv preprint arXiv:2408.02921.

12. Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI AI-based intrusion detection system. Measurement: Sensors, 28, 100827.

13. Katiyar, N., Tripathi, M. S., Kumar, M. P., Verma, M. S., Sahu, A. K., & Saxena, S. (2024). AI and Cyber-Security: Enhancing threat detection and response with machine learning. Educational Administration: Theory and Practice, 30(4), 6273-6282.

14. Jain, A., Bagoria, R., & Arora, P. (2025). An Intelligent Zero-day Attack Detection System using Unsupervised Machine Learning for enhancing Cybersecurity. Knowledge-Based Systems, 113833.

15. Touré, A., Imine, Y., Semnont, A., Delot, T., & Gallais, A. (2024). A framework for detecting zero-day exploits in network flows. Computer Networks, 248, 110476.

16. Zdrojewski, K. (2025). AI-Powered Cyberattacks: A Comprehensive Review and Analysis of Emerging Threats. Advances in IT and Electrical Engineering, 31, 55-70.

17. Laghari, A. A., Khan, A. A., Ksibi, A., Hajjej, F., Kryvinska, N., Almadhor, A.,& Alsubai, S. (2025). A novel and secure artificial intelligence-enabled zero-trust intrusion detection in an industrial Internet of Things architecture. Scientific Reports, 15(1), 26843.

18. Pinto, A., Herrera, L. C., Donoso, Y., & Gutiérrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. Sensors, 23(5), 2415.

19. Umba, S. M. W., Abu-Mahfouz, A. M., Ramotsoela, T. D., & Hancke, G. P. (2019, June). A review of artificial intelligence-based intrusion detection for software-defined wireless sensor networks. In 2019, IEEE 28th International Symposium on Industrial Electronics (ISIE) (pp. 1277-1282). IEEE.

20. Sunkara, G. (2022). AI-Driven Cybersecurity: Advancing Intelligent Threat Detection and Adaptive Network Security in the Era of Sophisticated Cyber Attacks. Well Testing Journal, 31(1), 185-198.

21. Jain, J. K., & Waoo, A. A. (2023). An artificial neural network technique for prediction of cyber-attacks using intrusion detection system. Journal of Artificial Intelligence, Machine Learning and Neural Network, 3(2), 33-42.

22. Alamro, H., Mansouri, W., Saeedi, K., Alshammeri, M., Aljabri, J., Alotaibi, F. A., & Sharif, M. M. (2024). Modelling of Bayesian-Based Optimized Transfer Learning Model for Cyber-Attack Detection in Internet of Things Assisted Resource Constrained Systems. IEEE Access.

BIOGRAPHIES

(Hemant Singh Patel is an M.Tech schola
Computer Science and Engineering at AK
University, Satna, Madhya Pradesh, curre
his third semester. His primary research f
on "AI-Powered Driven Intrusion System
Cyber Security and Zero-Day Attack
Detection," where he explores intelligent
techniques to identify novel threats and h
digital infrastructures. He is committed to
developing innovative solutions that mini
everyday hacking attempts and enhance t
reliability of networked systems. Alongsi
work, he has gained experience with a ra
emerging technologies, which supports a
practical understanding of modern compu
environments).