The Dual Role of AI in Cyber Security: Enhancing Ransomware and Defending Against Attacks

S. Sivalakshmi
Second year student Artificial Intelligence and Data Science
Arunai Engineering College
Tiruvannamalai, Tamilnadu, India
ssivalakshmi8126@gmail.com

Jayashree
Second year student Artificial Intelligence and Data Science
Arunai Engineering College
Tiruvannamalai, Tamilnadu, India
jayashreekathiresan07@gmail.com

S.Noorul Hassan
Assistant Professor Artificial Intelligence and Data Science
Arunai Engineering College
Tiruvannamalai, Tamilnadu, India
itsnoorul@gmail.com

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

I. INTRODUCTION

A. *The rise of Ransomware Attacks*

Ransomware attacks have evolved into a multi-billion-dollar criminal enterprise, with global damages estimated to exceed $20 billion in 2021 alone and projected to rise further in subsequent years. The ransomware business model is particularly attractive to cybercriminals because of its low-risk, high-reward nature. With the advent of crypto currencies like Bitcoin, criminals can demand ransoms with reduced risk of detection while ensuring anonymity during transactions. [17]

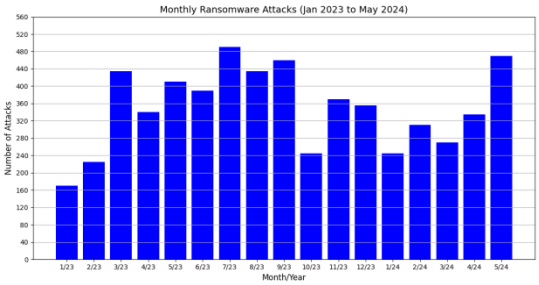

Fig.1 Ransomware attacks from Jan 2023 to May 2024

These assaults have increased in frequency due to Ransomware as a Service (RaaS), a business model in which cybercriminals rent or sell ransomware tools to non-technical customers. The issue has worsened with the democratization of ransomware, making it easier for inexperienced attackers to carry out complex operations. As a result, ransomware now targets large businesses, including healthcare systems, financial institutions, and essential infrastructure, rather than just individuals

B. *Economic and Social Impact of Ransomware*

The economic ramifications of ransomware attacks are staggering. In addition to ransom payments, organizations often face costs related to downtime, data loss, and reputational damage. For instance, the 2017 WannaCry ransomware attack crippled parts of the UK's National Health Service (NHS), delaying surgeries and costing millions in attackers' efforts. Similarly, the 2021 Colonial Pipeline attack caused widespread fuel shortages along the East Coast of the United States, highlighting the real-world consequences of ransomware on critical infrastructure.

Moreover, the rise in ransomware attacks during the COVID-19 pandemic illustrates the opportunistic nature of these cybercriminals. As organizations rushed to adopt remote work solutions, attackers exploited vulnerabilities in carelessly deployed networks and systems, further amplifying the scale and frequency of ransomware incidents.

C. *The Role of AI in Cyber Attacks*

Artificial intelligence (AI) has altered numerous industries, including cybersecurity, as AI is used by both attackers and defenders. Cybercriminals have leveraged AI's ability to automate and optimize several attack phases. Traditional malware uses static approaches, whereas AI-powered ransomware is dynamic and harder to detect and prevent.

Fig.2 Phishing

1) AI-Driven Phishing: One of the most effective techniques used in ransomware attacks is phishing, where attackers trick users into divulging sensitive information or downloading malicious software. AI-driven phishing elevates this threat by analyzing large volumes of communication patterns and personal data to craft more convincing and personalized phishing emails. This not only increases the likelihood of a successful attack but also helps ransomware spread more efficiently within targeted organizations. [2]

Example: In 2019, AI-driven phishing emails were reported by companies as indistinguishable from legitimate communications.

Attackers use AI to tailor their messages to the behaviors and communication styles of the individuals they targeted, significantly increasing the click-through rates of malicious links.

2) Automated Vulnerability Scanning: In addition to AI-driven phishing, cybercriminals use AI to automate vulnerability scanning—one of the critical steps in ransomware deployment. Vulnerability scanning traditionally involves identifying outdated software, misconfigured systems, or other weaknesses that can be exploited. With AI, this process becomes more efficient and thorough. AI models can analyze vast networks, identifying potential weaknesses in real-time, often faster than defenders can respond.

For example, attackers may use AI to scan large databases for systems running outdated versions of

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

software like Microsoft Windows, which could be exploited by ransomware such as WannaCry. Once vulnerabilities are identified, attackers can deploy ransomware quickly before patches are implemented. [3]

D. Defending against AI-Driven Ransomware

As ransomware evolves, so too must cybersecurity defenses. Traditional signature-based detection systems are increasingly unable to keep up with the dynamic nature of AI-enhanced malware. Signature-based detection relies on recognizing known patterns or 'signatures' of malicious software, which works well for static malware. However, AI-powered ransomware can alter its signature, rendering these traditional defenses ineffective. This is where "Intrusion Detection Systems (IDS)" and "Security Information and Event Management (SIEM)" come into play.

1) Intrusion Detection System: In addition to AI-driven phishing IDS monitors network traffic and system behaviors to identify potential threats. While traditional IDS can struggle to keep up with AI-powered ransomware, machine learning and AI-enhanced IDS offer a promising solution. By training AI models on large datasets of network activity, IDS can detect subtle patterns and anomalies that indicate the presence of ransomware. For example, AI-enhanced IDS can detect the unusually high file encryption activity associated with ransomware attacks, even when traditional malware signatures are missing. [4]

Fig.3 Intrusion Detection Systems

Furthermore, AI-enhanced IDS can adapt to evolving attack techniques. If ransomware changes its behavior to evade detection, machine learning models can be retrained to recognize new patterns, making these systems more resilient over time.

2) System Information and Event Management: SIEM systems gather and examine log data from all areas of an IT infrastructure within an enterprise. AI-enhanced SIEM is capable of processing massive volumes of data and identifying trends that could point to an upcoming assault in the context of ransomware defence. Artificial intelligence (AI)-based models are able to recognize abnormalities from "normal" system behavior, such as unexpected file access or strange network traffic, which could be signs of a ransomware attack.

For example, during the 2021 attack on Colonial Pipeline, suspicious network activity could have been identified early through advanced SIEM analytics, potentially allowing for faster mitigation of the attack.

E. Objectives of this paper

This paper aims to explore the evolving landscape of ransomware and the dual role of AI as both a tool for attackers and defenders. By focusing on the integration of AI in Intrusion Detection Systems (IDS), this research will:

1) Analyze how AI is being used to enhance ransomware capabilities, from phishing to encryption.

2) Assess the effectiveness of AI-enhanced IDS in detecting and mitigating ransomware attacks.

3) Explore real-world examples, such as "Ryuk" and "Maze", to illustrate the application of AI in both cyber attacks and defenses.

4) Provide insights and recommendations for future research directions to improve AI-based cybersecurity tools.

This research is critical in addressing the growing threat of ransomware and providing a roadmap for leveraging AI in the ongoing fight against cybercrime.

II. LITERATURE REVIEW

A. AI in Cyber Security

Artificial Intelligence (AI) is being more and more used in cybersecurity measures as researchers explore its potential to enhance offensive and defensive strategies. Research over the past ten years has concentrated on how AI may help defenses identify and instantly eliminate threats while also streamlining and improving various stages of cyber attacks. A significant examination by Parker and Bilimoria (2021), offers an extensive overview of machine learning techniques within cybersecurity. They accentuate the efficiency of supervised learning models like Support Vector Machines (SVM), Random Forest, and Neural Networks in recognizing attack patterns and detecting anomalies. Their work emphasizes the increasing significance of AI in forecasting zero-day attacks as well as dissecting intricate cyber threats that conventional systems struggle to uncover. [5]

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

Fig. 4 AI in Cyber Security

Cui et al. (2018) investigate deep learning methodologies for identifying cyber hazards, highlighting the proficiency of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in analyzing vast datasets and recognizing nuanced patterns indicative of malicious activities. Collectively, these findings lay the groundwork for embracing AI in cybersecurity frameworks, particularly in network intrusion detection and threat assessment. [6]

B. Evolution of Ransomware and AI integration

Li et al. (2021) explore the evolution of ransomware attacks that incorporate Al strategies to improve encryption, automate phishing, and evade detection. They emphasize how Al-powered ransomware, such as Ryuk and Maze, uses machine learning algorithms to dynamically adjust attack strategies, making it more difficult for traditional antivirus tools to detect and counteract these attacks.[7]

Furthermore, research by Kumar and Sangwan et al. (2012) illustrates AI's function in enabling ransomware to adjust to different scenarios. Attackers leverage machine learning techniques to pinpoint high-value targets, prioritize data for encryption, and tailor ransom requests according to the financial capabilities of victims. These advancements pose an escalating challenge for defenders who depend on static signature-based detection systems. [8]

C. Integration Intrusion Detection System (IDS) with AI

Intrusion Detection Systems (IDS) have historically been pivotal in network security, primarily tasked with identifying nefarious activities through established protocols. However, conventional IDS solutions have faced difficulties keeping up with the rising sophistication of cyber threats. This disparity has prompted the infusion of AI into IDS architectures, empowering these systems to learn from historical data and recognize novel threats in real time

Research by Jadhav and Channe et al. (2016) investigates how machine learning optimizes IDS performance, concentrating on algorithms such as k-Nearest Neighbors (k-NN) Decision Trees and Naive Bayes in their findings indicate that AI-augmented IDS systems can accurately detect a variety of threats, including ransomware incursions. The flexibility of AI facilitates the evolution of these systems as new risks emerge, considerably decreasing detection times. [9]

Further inquiries by Boukhalfa et al. (2020) assess deep learning frameworks like auto encoders and LSTMs (Long Short-Term Memory networks) for anomaly-based IDS. They demonstrate that deep learning models are adept at processing extensive volumes of network traffic, identifying even subtle signs of ransomware attacks. This enhances threats rather than merely reacting post-attack. [10]

D. Security Information and Event Management with AI

Security Information and Event Management (SIEM) systems have become increasingly significant in recent years, serving as centralized hubs for collecting, analyzing, and responding to security incidents across diverse environments. Traditional SIEM frameworks frequently depend on rule-based detection, which may prove inefficient against more sophisticated and elusive attacks like AI-driven ransomware. Consequently, researchers are looking towards AI to bolster SIEM system functionalities.

In a study by Laue et al. (2021), the capability of AI-enhanced SIEM systems in identifying intricate ransomware attacks was evaluated. Their results indicate that AI models, such as anomaly detection methods and neural networks, empower SIEM systems to process vast quantities of event data in real-time, recognizing attack patterns that might otherwise escape human notice. This approach is particularly beneficial for ransomware identification, where early indications of infection (such as unusual file access behaviors or rapid encryption actions) can be detected before the attack propagates. [11]

Additionally, Ban et al. (2023) explore the application of reinforcement learning in SIEM systems to automate threat responses. Their findings reveal that AI-driven SIEM platforms not only enhance detection precision but also streamline incident response times, thus mitigating the overarching effects of ransomware assaults. [12]

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

III. Materials and Methods

A. Specific IDS model

In this study, we concentrate on the Network Intrusion Detection System (NIDS), specifically exercising the Snort IDS. The widely recognized open-source IDS is Snort, known for its real-time traffic analysis, packet logging, and customizable rule-based detection of various attacks. It operates on the principles of both hand-grounded and anomaly-grounded discovery methodologies to give comprehensive trouble discovery.

1) Signature Grounded Discovery:Snort's Signature-grounded discovery involves comparing network business against a set of predefined attack autographs. These signatures are patterns or byte sequences that represent known malicious activities. For example, Snort can identify common ransomware behaviors, such as known command and control (C2) business or specific loads used in ransomware attacks. This system is highly effective for relating known pitfalls but may struggle with new or variant ransomware strains that don't match being autographs.[13

2) Anomaly Grounded Discovery:To round signature-grounded discovery, Snort employs anomaly-grounded discovery. This approach involves establishing a baseline of normal network behaviors and monitoring for diversions from this behavior. Anomalies such as unanticipated spikes in encryption activities or unusual train access patterns are flagged as implicit pitfalls. This system allows Snort to detect new or modified ransomware strains that don't have known autographs but parade abnormal behavior. [14]

B. *Implementation of IDS models:*

The Snort IDS is configured with custom rules acclimatized to descry ransomware-specific actions. [18] The configuration process involves:

1) *Rule Creation:* Developing specific Snort rules to descry ransomware- related conditioning. For example, rules might include patterns reflective of ransomware encryption processes or C2 dispatches.
2) *Rule Tuning:* Conforming the perceptivity of rules to balance between detecting factual pitfalls and minimizing false cons. This involves fine-tuning thresholds and parameters grounded on network business patterns.
3) *Testing and confirmation:* assessing the effectiveness of the configured IDS by bluffing ransomware attacks in a controlled terrain. This helps insure that the IDS rules directly identify ransomware and don't induce inordinate false cons.

C. How AI powered IDS detects ransomware:

AI-powered IDS represents an advanced evolution of traditional IDS by incorporating machine learning (ML) and deep learning (DL) methods. [4] These AI techniques enhance the IDS's capability to detect sophisticated threats like ransomware, which may bypass traditional detection methods. Machine Learning Models: Developing specific Snort rules to detect ransomware Models AI-powered IDS employs ML algorithms to classify network business as:

1) Random Forest: An ensemble learning method that aggregates results from multiple decision trees to improve classification accuracy. It handles various data patterns and detects complex ransomware. [32]
2) Support Vector Machines: A classification algorithm that finds the optimal hyper plane to separate classes. SVM is versatile. [32]
3) Gradient Boosting Machine: An ensemble system that builds models successively, correcting the **errors** of former models. GBM can enhance detection accuracy by **focusing** on **difficult-to-classify** samples.[33]

D. Deep Learning Models:

For further complex pattern recognition, AI-powered IDS integrates DL models such as:

1) Convolution Neural Networks: Used for pattern recognition. CNNs can analyze network traffic for intricate patterns and anomalies indicative of ransomware.[6]
2) Recurrent Neural Networks: Particularly useful for sequential data, RNNs can track changes in network behavior over time, helping to identify ransomware conditionings that involve timed or sequential encryption operations.[15]

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

E. Discovery Process:

1) *Data Collection*: The AI- powered IDS collects comprehensive network business data, including packet heads, loads, and metadata. [19]

2) *Feature Extraction*: Applicable features for ransomware discovery are uprooted from the collected data. These features may include criteria like packet sizes, inter-arrival times, and encryption patterns.[31]

3) *Model Training and Conclusion*: The uprooted features are fed into AI models. During training, these models learn to classify network business grounded on patterns reflective of ransomware. Once trained, the models are used to make real-time consequences about incoming network business.[32]

4) *Alert Generation*: When the AI- powered IDS detects patterns or anomalies harmonious with ransomware behavior, it generates cautions. These cautions give detailed information on implicit pitfalls, including the nature of the suspicious exertion and suggested response conduct.

F. How IDS deals with AI

Integration of AI in IDS: Integrating AI into IDS involves several crucial advancements that ameliorate the system's capability to descry and respond to ransomware pitfalls.

1) *Adaptive learning*: AI- powered IDS continuously learns and adapts to new crypto Trojan variants. This involves regularly streamlining AI models with new training data that includes recent ransomware attack patterns. Adaptive literacy ensures that the IDS remain effective against evolving pitfalls.[20]

2) *Behavioural Analysis*: AI ways enable behavioural analysis of network business. By examining diversions from established morals, AI- powered IDS can identify ransomware conditioning similar as unusual encryption processes or train variations that diverge from typical stoner behaviour.[21]

3) *Multi-Layered Discovery:* AI enhances traditional discovery styles by adding fresh layers of analysis. For case, while hand-grounded discovery might identify known ransomware, AI models can descry new ransomware strains by feting behavioural patterns not preliminarily seen.

4) *Continuous Enhancement:* AI can facilitate ongoing advancements in IDS performance through:

5) *Model Retraining:* AI models are periodically retrained with updated data to enhance their accuracy. This process involves incorporating feedback from detected incidents and enriching the models to better distinguish between benign and malicious traffic.

6) *Feedback Loops*: Implementing feedback loops allows the IDS to incorporate information from previous findings and responses. This iterative process helps to upgrade detection algorithms and improve overall system performance. [22]

F. Data Sources:

1) The CICIDS Dataset: The Canadian Institute for Cybersecurity Intrusion Detection System (CICIDS) dataset is employed for training and assessing AI models. This dataset contains label cases of colourful network business types, including ransomware attacks. It provides a comprehensive resource for developing and testing IDS models. [23]

2*) AI-Models*: Implementing machine learning and deep learning models is easy with libraries like Scikit-Learn, TensorFlow, and PyTorch. These libraries offer tools and fabrics for structuring, training, and assessing AI models. [24]

By evolving on these aspects, this section provides a detailed and comprehensive explanation of the accoutrements and styles used in the study, enhancing the understanding of how IDS and AI ways are employed to descry and alleviate ransomware pitfalls.

An artificial intelligence (AI language model (ChatGPT, OpenAI) was employed to help as a writing guide, and help with content organization for coherence and clarity during the drafting process. The authors completed all intellectual content and final revisions; the AI tool was a supplemental resource.

Canva, a graphic design platform with an intuitive interface for producing high-quality pictures, and Crayon, an AI-powered image-generating tool, were used in this study to create the images. These resources were essential in creating the visual content that was reported in this study

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

IV. Results and Proposed Framework

In this section, we will outline a proposed framework for how AI-powered Intrusion Detection Systems (IDS) to combat ransomware attacks. We'll focus on the AI models used, how the system handles data, and how ransomware is detected, and explore a step-by-step method to implement and evaluate the system.

Key Components:

A. *Data mining and Preprocessing:* Network traffic, system logs, and user activity are collected.
B. *Feature Extraction:* Relevant features are extracted from the data using statistical analysis and AI algorithms.
C. *AI-Based Detection*: Machine learning and deep learning models analyze the features to detect potential ransomware attacks.
D. *Threat Response*: Upon detecting a threat, the IDS alerts administrators and, in some cases, automatically initiates countermeasures like isolating infected systems.
E. *Continuous Learning*: The system adapts to new threats by retraining models with new data over time.

A. Data Collection and Preprocessing: The first step involves collecting a large amount of network traffic and log data from monitored systems. [19]

Fig.5 Data collection

These data points will be the foundation of the framework:

1) *Network Traffic*: Data packets, source IPs, destination IPs, protocol types, etc.
2) *System Logs*: Authentication logs, file access logs, and error reports.
3) *User Behavior Logs*: Data on login frequency, data access patterns, and file transfers. This raw data is often too large and noisy for immediate use in an AI model. Therefore, data preprocessing is crucial to prepare it for analysis:
4) *Data Cleaning*: Remove missing or inconsistent data.
5) *Feature Engineering*: Extract critical attributes like network flow characteristics, encryption behavior, and suspicious file operations.

B. *Feature Extraction*: To make the AI model effective, relevant features are extracted from the data. [31] Some features that can be crucial in ransomware detection include:

1) *Frequency of network anomalies*: Abrupt increases in outgoing traffic may indicate the presence of data eavesdropping.
2) *Encryption behavior*: AI can monitor files for abnormal encryption activity or changes in file extensions.
3) *User activity monitoring*: Questionable actions, such a string of unsuccessful login attempts or huge file transfers, could be signs that ransomware is attempting to access private data.

C. AI Powered Detection systems:

1) *Supervised Learning*: AI models such as Support Vector Machines (SVM) or Decision Trees are trained on labeled datasets to classify incoming data. However, supervised learning has limitations when dealing with novel attacks for which no labeled data is available.[29]
2) *Unsupervised Learning:* Models like K-Means clustering or Gaussian Mixture Models (GMM) can detect anomalies by clustering norm traffic data.

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

Anything that falls outside the norm (i.e., new, unexpected ransomware behavior) triggers an alert. [29]

3) *Deep Learning Models*: Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) are increasingly being applied to IDSs.[6]

D. Dealing with AI Techniques in Ransomware: Modern ransomware attacks are often AI-enhanced, employing techniques such as polymorphic code, AI-driven phishing, and automated encryption. [27] The proposed IDS need to counteract these sophisticated strategies:

1) *Detecting Polymorphic Ransomware*: By using deep learning techniques, the system can analyze slight changes in malware code, even if the ransomware frequently modifies its signature.
2) *Countering AI-Driven Phishing*: Natural language models like BERT (Bidirectional Encoder Representations from Transformers) can analyze email text to flag AI-generated phishing attempts.

E. Response mechanisms: The IDS includes both passive and active response mechanisms:

1) *Passive Responses:* Alerts and logging suspicious activities for further analysis.
2) *Active Responses*: Blocking IPs, isolating compromised systems, or stopping file encryption processes. Active responses can be automatic, based on confidence thresholds from the AI model predictions.[28]

F. Evaluation Metrics: Evaluating the effectiveness of the AI-IDS involves measuring:

1) *Accuracy*: How many ransomware attacks the system detects correctly.
2) *False Positives*: How often legitimate activity is mistakenly flagged as ransomware.
3) *Time to Detection*: How fast the system can detect ransomware compared to traditional IDSs.
4) *Adaptability*: The ability of the AI-IDS to recognize new and evolving ransomware techniques.

G. Continuous Learning and Model Updates: As new ransomware strains emerge, the IDS can continuously improve through machine learning updates. This involves regularly retraining the AI models with new data, ensuring that the system remains robust against the latest attack methods. [30]

V. Discussions, Limitations and Future Directions

These sections discuss the drawbacks and difficulties that AI-based intrusion detection systems (IDS) must overcome in order to successfully combat ransomware attacks. When IDSs and AI are paired, they offer sophisticated methods for spotting unusual network activity that might be a symptom of a ransomware assault. However, standard IDS methods frequently cannot keep up with the sophistication of ransomware, necessitating a dynamic and developing strategy that makes use of machine learning (ML) and artificial intelligence (AI) capabilities.

A. Effectiveness of AI-based IDSs in Ransomware Detection: AI-based IDSs offer several key advantages over traditional systems when it comes to detecting ransomware. Machine learning models can recognize patterns in massive amounts of data and detect ransomware activity at an early stage. This is important because of the rise of polymorphic ransomware that constantly changes its code to become undetectable. Traditional IDS systems rely on manual indexing and are ineffective against these attacks. However, AI-based systems can detect behavioral errors and adapt better to new threats. [14]

For example, techniques such as anomaly detection and unsupervised learning allow IDSs to detect deviations from normal behavior that indicate an incoming ransomware attack. These models are trained on normal network behavior, and anything that deviates from this schedule will trigger an alert, even if the ransomware is new and doesn't have a specific brand.AI-based neural networks and deep learning models have also proven effective at detecting even the smallest changes in network traffic, improving the ability of IDS systems to detect ransomware attacks before serious damage occurs. These systems learn over time, improving their detection rates as more data is fed into the model. [25]

B. AI Techniques for evasion of detection: While AI is improving the detection capabilities of IDSs, ransomware authors are also starting to use AI to evade detection. AI obfuscation techniques, where malware continually changes its signatures and behaviors, pose a challenge to both traditional and AI-based IDSs. This creates a constant cat-and-mouse game where ransomware evolves as IDSs become more capable. Another problem is false

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]

positives and false negatives. AI-based IDS models can sometimes flag legitimate activity as suspicious (false positive) or miss genuine ransomware attacks (false positive). [26]

C. Addressing limitations and Challenges: Current research focuses on merging diverse detection approaches, such as behavioral analysis and brand-based search, in order to increase the accuracy and efficiency of AI-based IDSs [27]. Accurate recognition can be increased by hybrid models that combine machine learning and rule systems. Furthermore, the integration of SIEM (Security Information and Event Management) systems with IDS is becoming more and more important. SIEM can connect events and analyze data from various sources to offer a more comprehensive picture of possible dangers. SIEM can lessen false positives and increase detection accuracy by combining data from IDS with data from other security technologies. [17]

D. Future References: To keep pace with increasingly sophisticated ransomware attacks, future IDS research and development should focus on the use of advanced AI techniques such as reinforcement learning and adversarial machine learning. These techniques can help security systems predict potential attack vectors before ransomware infiltrates a system. IDS can play an important role in detecting and mitigating ransomware by integrating artificial intelligence into various layers of cyber security, but it needs to be constantly improved to respond to new threats. [16]

VI. Conclusion

Artificial Intelligence (AI) transforms cybersecurity by refining both offensive techniques and protective measures. Advanced Intrusion Detection Systems (IDS) utilizing Artificial Intelligence (AI) detect and mitigate threats effectively. Constant Innovation is essential to address the rapidly changing challenges within the cybersecurity domain.

References

[1] K. K. Gagneja, "Knowing the ransomware and building defense against it—specific to healthcare institutes," in Proc. 2017 Third Int. Conf. Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2017, pp. 1-5, doi: 10.1109/MOBISECSERV.2017.7886569.

[2] Muhammad Mudassar Yamin, Mohib Ullah, Habib Ullah, Basel Katt, "Weaponized AI for cyber Attacks", Journal of information security and applications, vol.57, art.no 102722, March 2021.

[3] H.J. Liao, C.H. R. Lin, Y.C. Lin, and K.Y. Tung, "Intrusion detection system: A comprehensive review," J. Network Comput. Appl., vol. 36, no. 1, pp. 16-24, 2013.

[4] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of deep learning to real-time web intrusion detection," IEEE Access, vol. 8, pp. 70245-70261, 2020.

[5] P. Parkar and A. Bilimoria, "A survey on cyber security IDS using ML methods," in Proc. 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 352-360.

[6] J. Cui, J. Long, E. Min, Q. Liu, and Q. Li, "Comparative study of CNN and RNN for deep learning based intrusion detection system," in Cloud Computing and Security: 4th International Conference, ICCCS 2018, Haikou, China, June 8-10, 2018, Revised Selected Papers, Part V, vol. 4, pp. 159-170, 2018.

[7] V. Kumar and O. P. Sangwan, "Signature based intrusion detection system using SNORT," Int. J. Comput. Appl. Inf. Technol., vol. 1, no. 3, pp. 35-41, 2012

[8] A. S. Li, "An analysis of the recent ransomware families," Project Report, Purdue University, 2021.

[9] S. D. Jadhav and H. P. Channe, "Comparative study of K-NN, naive Bayes and decision tree classification techniques," Int. J. Sci. Res. (IJSR), vol. 5, no. 1, pp. 1842-1845, 2016.

[10] A. Boukhalfa, A. Abdellaoui, N. Hmina, and H. Chaoui, "LSTM deep learning method for network intrusion detection system," Int. J. Electr. Comput. Eng., vol. 10, no. 3, pp. 3315, 2020.

[11] T. Laue, C. Kleiner, K.-O. Detken, and T. Klecker, "A SIEM architecture for multidimensional anomaly detection," in Proc. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1, pp. 136-142, 2021.

[12] T. Ban, T. Takahashi, S. Ndichu, and D. Inoue, "Breaking alert fatigue: AI-assisted SIEM framework for effective incident response," Appl. Sci., vol. 13, no. 11, p. 6610, 2023.

[13] S. Chakrabarti, M. Chakraborty, and I. Mukhopadhyay, "Study of snort-based IDS," in Proc. Int. Conf. Workshop Emerging Trends Technol., 2010, pp. 43-47.

[14] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert Systems with Applications, vol. 29, no. 4, pp. 713-722, 2005.

[15] X. Zhang, C. Wang, R. Liu, and S. Yang, "Federated RNN-based detection of ransomware attacks: A privacy-preserving approach," OSF, 2024.

[16] Y. Hamid, M. Sugumaran, and V. R. Balasaraswathi, "IDS using machine learning—current state of art and future directions," Brit. J. Appl. Sci. Technol., vol. 15, no. 3, pp. 1-22, 2016.

[17] S. Kamil, H. S. Abdullah, S. N. Ahmad Firdaus, and O. L. Usman, "The rise of ransomware: A review of attacks, detection techniques, and future challenges," in 2022 International Conference on Business Analytics for Technology and Security (ICBATS), 2022, pp. 1–7.

[18] M. Saber, S. Chadli, M. Emharraf, and I. El Farissi, "Modeling and implementation approach to evaluate the intrusion detection system," in Networked Systems: Third International Conference, NETYS 2015, Agadir, Morocco, May 13-15, 2015, Revised Selected Papers, vol. 3, 2015, pp. 513–517.

[19] B. Molina-Coronado, U. Mori, A. Mendiburu, and J. Miguel-Alonso, "Survey of network intrusion detection

methods from the perspective of the knowledge discovery in databases process," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2451–2479, Dec. 2020

[20] A. Chiche and M. Meshesha, "Towards a scalable and adaptive learning approach for network intrusion detection," Journal of Computer Networks and Communications, vol. 2021, no. 1, p. 8845540, 2021.

[21] D. Moon, H. Im, I. Kim, and J. H. Park, "DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks," The Journal of Supercomputing, vol. 73, pp. 2881–2895, Jul. 2017.

[22] B. J. Asaju, "Advancements in Intrusion Detection Systems for V2X: Leveraging AI and ML for Real-Time Cyber Threat Mitigation," Journal of Computational Intelligence and Robotics, vol. 4, no. 1, pp. 33-50, 2024.

[23] D. Stiawan, M. Y. B. Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 dataset feature analysis with information gain for anomaly detection," IEEE Access, vol. 8, pp. 132911–132921, 2020.

[24] İ. Avcı and M. Koca, "Cybersecurity attack detection model, using machine learning techniques," Acta Polytechnica Hungarica, vol. 20, no. 7, pp. 29–44, 2023.

[25] L. Fritsch, A. Jaber, and A. Yazidi, "An overview of artificial intelligence used in malware," in Symposium of the Norwegian AI Society, 2022, pp. 41–51.

[26] S. Poudyal and D. Dasgupta, "AI-powered ransomware detection framework," in 2020 IEEE Symposium Series on Computational Intelligence (SSCI), 2020, pp. 1154–1161.

[27] G. Kumar, K. Kumar, and M. Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: a review," Artificial Intelligence Review, vol. 34, pp. 369–387, Dec. 2010.

[28] W. T. Yue and M. Çakanyıldırım, "A cost-based analysis of intrusion detection system configuration under active or passive response," Decision Support Systems, vol. 50, no. 1, pp. 21–31, Nov. 2010.

[29] P. Laskov, P. Düssel, C. Schäfer, and K. Rieck, "Learning intrusion detection: supervised or unsupervised?," in Image Analysis and Processing – ICIAP 2005: 13th International Conference, Cagliari, Italy, September 6-8, 2005, Proceedings, vol. 13, 2005, pp. 50–57.

[30] X. He, Q. Chen, L. Tang, W. Wang, T. Liu, L. Li, Q. Liu, and J. Luo, "Federated continuous learning based on stacked broad learning system assisted by digital twin networks: An incremental learning approach for intrusion detection in UAV networks," IEEE Internet of Things Journal, vol. 10, no. 22, pp. 19825-19838, 2023.

[31] M. Sato, H. Yamaki, and H. Takakura, "Unknown attacks detection using feature extraction from anomaly-based IDS alerts," in 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, 2012, pp. 273-277.

[32] M. A. M. Hasan, M. Nasser, B. Pal, and S. Ahmad, "Support vector machine and random forest modeling for intrusion detection system (IDS)," Journal of Intelligent Learning Systems and Applications, 2014.

[33] B. A. Tama and K.-H. Rhee, "An in-depth experimental study of anomaly detection using gradient boosted machine," Neural Computing and Applications, vol. 31, pp. 955-965, 2019.

DOA:20.01.2025 / DOP: 27.01.2025 ISSN: 3048-619X
Volume 1 Issue 3 [Jan – Apr 2025]