IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13633

A Survey on Next Generation Intrusion Detection Systems Empowering Advanced Threat Detection with Generative AI

Akshata Bhadti[1], Dr Pijush Barthakur[2]

Student, Department of MCA, K. L. S. Gogte Institute of Technology, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[1]

Professor, Department of MCA, K. L. S. Gogte Institute of Technology, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[2]

Abstract: Intrusion Detection Systems (IDSs) have been crucial in protecting computer networks from malicious activities. However, with the rapid evolution of cyber threats and the increasing complexity of network architectures, traditional IDSs are insufficient for effectively detecting and preventing modern attacks. Next Generation Intrusion Detection Systems (NG-IDSs) have emerged in response to these challenges, incorporating advanced technologies to enhance detection capabilities and improve overall security. This survey provides an overview highlighting the key features, applications in diverse networks, and discussing current challenges. It uniquely examines the integration of Generative AI (Gen AI) within IDS frameworks, focusing on Generative Adversarial Networks (GANs) to create synthetic data and emulate complex attack patterns, significantly enhancing the detection of previously unseen threats. Additionally, the survey explores the use of ChatGPT for real-time threat alerts and Large Language Models (LLMs) like GPT-4 in protecting critical infrastructures such as energy grids. This survey aims to offer valuable insights by identifying the challenges and limitations faced by NG-IDSs and proposing areas for future research and development.

Keywords: AI, ChatGPT, IDS, intrusion detection system, Generative Adversarial Networks, Generative AI, models, datasets, IoT, security, social engineering, LLM

I. INTRODUCTION

In the rapidly evolving landscape of cybersecurity, the need for robust intrusion detection systems (IDS) has become increasingly paramount. Traditional IDS, reliant on signature-based and anomaly-based detection methods, are facing challenges in effectively identifying and mitigating sophisticated cyber threats. As adversaries continue to develop more sophisticated attack strategies, there arises a pressing need for next-generation IDS that can adapt and respond to these evolving threats in real-time. By harnessing the power of generative AI, IDS can potentially revolutionize the way threats are identified, analyzed, and neutralized. Generative AI, encompassing techniques such as Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), enables the creation of synthetic data and the emulation of complex patterns and behaviors. Using generative AI within IDS opens up new avenues for detecting and pre-empting previously unseen threats, augmenting the ability to proactively defend against cyber intrusions. The emergence of Generative Artificial Intelligence (GAI) is for enhancing the capabilities of next-generation IDS, enabling more advanced threat detection and mitigation strategies.

II. LITERATURE REVIEW

The integration of generative AI in cybersecurity has garnered significant attention in recent years due to its potential to enhance threat detection capabilities. This literature review will display the works done to date in the area, initial outcomes, and challenges, at the same time that the gaps in knowledge to be faced by future research will be delimited.

2.1 Current Research

Generative AI models, such as Generative Adversarial Networks (GANs), have been employed to generate synthetic IoT data that can be used to train ML models. The Current study is further positioned to derive solution models based on ML for adequate detection and protection against its diversified forms of security threats in IoT.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024
DOI: 10.17148/IJARCCE.2024.13633

These solutions are intended based on the power of generative AI models for the synthesis of imitated IoT data, with the potential of training the ML models in solving such peculiar challenges of security for IoT. The use of ML and DL techniques for AI-based intrusion detection systems has been the focus of several approaches and models in cybersecurity literature. For example, it is yet to be established how well these would do in real-world situations over and above what currently they are being presented within literature.

2.2 Integrating ChatGPT with Intrusion Detection Systems

One can integrate ChatGPT with intrusion detection systems to provide real-time alerts and notifications, given that a potential threat has been identified. Here, natural language descriptions of patterns and behaviors correlated with attacks are derived by analyzing the security-related data. With the help of behavior, patterns, and trends of activities—both historical and current —associated with the threats, ChatGPT learns to develop rules and policies for advanced Intrusion Detection that can effectively respond to new threats. Thus, the synergy between Generative AI and IoT security will handle the recent area of intensive research in the context of integrations in ML. Other applications concerning generative models based on generative AI, such as GANs, include generating synthetic data that adheres to the generative AI training procedure for ML IoT models. It, therefore, becomes possible to come up with ML models that are very accurate, using much robustness to give solutions capable of taking up unique challenges in the IoT era, such as data scarcity and real-time processing. This makes a study of the synergy between generative AI and cybersecurity a critical one, with far-reaching implications for the future of cybersecurity.

2.3 Identification of gaps

One significant gap is the limited focus on the adopted AI techniques, which often lacks in-depth analysis of AI-based detection techniques, review of benchmark datasets, result evaluation, feature importance to detect different attacks, and threats to AI-based models. The research on in-vehicle networks (IVNs) using AI-based intrusion detection systems highlights gaps in the existing literature. The lack of comprehensive surveys that cover the entire spectrum of AI-based IDSs for IVNs, including their detection features and algorithms, is another gap. The existing literature often fails to discuss the security of AI models, necessary steps to develop AI-based IDSs in the CAN bus, and identifies limitations of existing proposals. These gaps highlight the need for more comprehensive and in-depth research in this area to develop more effective and robust AI-based IDSs for IVNs.

III. CAUSES AND CHALLENGES

The primary cause for employing AI-based techniques in Intrusion Detection Systems (IDS) is the increasing frequency of cyber-attacks. Some causes driving the adoption of AI in IDS include:

1. Complexity of Cyber Threats: Cyber-attacks are becoming more sophisticated, involving advanced techniques such as zero-day exploits, ransomware, and social engineering. AI-based IDS can adapt to these complex threats by continuously learning from new data and evolving attack patterns.
2. Data Imbalance: Most network traffic is benign, with malicious behavior occurring rarely. This imbalance poses a challenge for traditional IDS models, which struggle to detect rare attack types accurately. AI algorithms can handle imbalanced datasets more effectively by learning from the available data and identifying anomalies.
3. Scalability Issues: Traditional IDS models are often unable to scale effectively to handle large volumes of network traffic data. AI-based techniques, particularly deep learning models, can process and analyze vast amounts of data in real-time, enabling IDS to scale to meet the demands of modern networks.
4. Adversarial Attacks: Adversaries may attempt to deceive AI-based IDS by manipulating the training data or exploiting algorithmic vulnerabilities. Researchers are exploring techniques like adversarial training and explainable AI to make AI-based IDS more robust against such attacks.
5. Data Quality and Bias: Ensuring high-quality, unbiased data is crucial for the effective training of AI models. Techniques like feature selection and data augmentation can help improve the quality and diversity of the data used to train AI-based IDS.
6. Privacy and Ethical Concerns: AI-based threat detection involves processing sensitive data, raising privacy and ethical issues that need to be addressed. Researchers are exploring privacy-preserving techniques and developing guidelines to ensure the responsible development and deployment of AI-based IDS.

AI algorithms can analyze contextual information, such as recent events, social connections, and online activities, to craft messages that are relevant and timely. By incorporating contextual cues into social engineering attacks, attackers can increase the effectiveness of their campaigns and make them more convincing to the target audience.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024
DOI: 10.17148/IJARCCE.2024.13633

Deception and Manipulation techniques where AI technologies, such as deepfakes, can create realistic audio or video content that deceives individuals by mimicking someone's appearance and voice. This allows attackers to manipulate targets into believing false information or taking malicious actions based on fabricated content. AI-driven tools enable attackers to automate the creation and dissemination of social engineering messages, increasing the scalability of their campaigns. With AI for content generation, attackers can reach a larger audience and conduct multiple attacks simultaneously with minimal manual effort.

IV. DATASETS AND MODELS

4.1 Large Language Models

Generative AI, particularly Large Language Models (LLMs) like GPT-4, presents significant potential in enhancing cybersecurity measures within critical infrastructure such as energy grids. These models can analyze unstructured data from various sources like online forums and system logs to detect and predict cyber threats, including phishing attacks and malware targeting energy systems. However, concerns about data privacy arise when processing such sensitive information in external data centers. Developing sector-specific LLMs deployed within a company's data center can mitigate these risks and enhance data protection.

Integrating Retrieval Augmented Generation (RAG) technology into Critical Infrastructure Protection (CIP) offers a transformative approach. RAG combines information retrieval with text generation, enabling real-time access to external databases and up-to-date threat intelligence. This approach ensures contextually relevant and accurate responses, crucial for safeguarding critical assets such as power grids, water systems, and communication networks against evolving cyber threats.

Table 4.2: LLMs mentioned in the survey with their features and descriptions

LLM	Features/Description
ChatGPT	Versatile in text generation, language translation, question answering; understands code semantics, identifies security vulnerabilities.
Bard	Similar to ChatGPT, versatile in text generation and language-related tasks.
Google LaMDA	Detects and watermarks AI-generated text, useful for identifying phishing emails and polymorphic codes.
GPT-4	Analyzes and interprets extensive unstructured text data to predict and identify potential cyber threats in the energy sector.
LLaMA 2-Chat	Evaluated for human safety, effective in comparing - understanding complex tasks.
MPT	Model tested for human safety, provides robust analysis capabilities.
Vicuna	Used in human safety evaluations, capable of in-depth understanding and analysis.
Falcon	Focuses on comprehensive analysis and understanding.
PaLM	Effectiveness in human safety, demonstrates robust analytical capabilities

In cybersecurity, these models are increasingly used to detect security vulnerabilities and mitigate risks. For instance, LLMs trained on extensive datasets can analyze code semantics to identify potential vulnerabilities in software. They can also be employed to detect and watermark AI-generated text used in cyberattacks, such as phishing emails or polymorphic codes. By generating synthetic malware samples, LLMs assist in testing and evaluating malware detection systems, enhancing their effectiveness against diverse malware variants. Moreover, in network security, LLMs can model normal network behavior to detect anomalies indicative of security breaches or intrusions. They are also applied in monitoring blockchain activities to identify suspicious patterns and ensure data integrity through digital signatures and consistency verification across distributed nodes. However, challenges such as perpetuating biases from training data remain a concern, necessitating careful consideration in deploying LLMs for cybersecurity applications.

4.3 Dataset Characteristics and Analysis

The effectiveness of AI-based IDS depends on the quality and diversity of the datasets used for training and evaluation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13633

Table 4.4 Various datasets used in the analysis across the survey

Dataset	Description	Use Cases	Key Features	Conclusion
NSL-KDD Dataset	A widely used dataset in IDS research, providing a comprehensive set of network traffic data, including both benign and malicious activities.	Evaluation of IDS models, anomaly detection research	Comprehensive data including both benign and malicious activities.	Addresses issues in the original KDD dataset, such as duplicate records and data structure issues.
UNSW-NB15 Dataset	A modern dataset that includes a diverse set of network traffic data, with both normal and malicious traffic.	Performance evaluation of AI-based NIDS models	Diverse network traffic data, successor to NSL-KDD dataset.	Provides more realistic and comprehensive traffic scenarios compared to NSL-KDD.
CIC-IDS Dataset	Contains real-time network traffic data, including various types of attacks such as DoS, DDoS, and infiltration.	Training machine learning models, developing IDS schemes	Real-time traffic data, various attack types including DoS, DDoS, and infiltration attacks.	Popular for its detailed and realistic network traffic data.
KDD'99 Dataset	IDS using ANN trained on any database with high accuracy.	Intrusion detection in CPS.	GAN-generated training data, improved accuracy, handles data error	G-IDS outperforms standalone IDS (S-IDS).
KDD and NSL-KDD	Widely-used datasets for evaluating IDS, containing network intrusion data.	Evaluating and benchmarking IDS performance.	Comprehensive, well-labeled, includes various attack types.	High accuracy achieved with models using GAN and LSTM.
Virus Share APK Android malware & BIG-2015	Combined datasets used for malware detection and classification.	Malware detection and classification.	Robustness, ability to generalize from limited data.	Mal-IAGAN model achieved over 80% accuracy with only 1% of the dataset.
IoT-23	A dataset from IoT devices, includes 20 malicious and 3 benign sub-datasets, used in evaluating IDS.	Intrusion detection in IoT environments.	Contains 23,145 network flows categorized into Benign, C&C, DDoS, and PortScan.	Effective in detecting various types of threats in IoT scenarios.
UNSW-NB15	Dataset for evaluating IDS, contains network traffic with a mix of normal & malicious activities.	Network intrusion detection.	Comprehensive, diverse attack types, realistic traffic.	Used to test and validate IDS models.
CIP-RAG	CIP dataset using RAG to enhance security for critical assets like power grids and water systems.	Protecting critical infrastructure, detecting cyber-attacks in energy sectors.	Combines retrieval component with text generation for real-time, contextually relevant responses.	Enhances accuracy and relevancy of threat detection, addresses privacy concerns with sector-specific models
Google Home Mini Dataset	Dataset created from Google Home Mini, used for intrusion detection tasks.	Intrusion detection, data generation, and augmentation.	Contains sequences of packets, with a vocabulary size of 535.	Effective in generating realistic samples using GAN.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13633

V. PRACTICAL IMPLEMENTATION

5.1 Implications of AI-generated Content in Cyber Attacks

In traditional network IDS, machine learning models often use GANs to enhance performance. For instance, in one study, the Deep Convolutional Generative Adversarial Network (DCGAN) and Long Short-Term Memory (LSTM) methods were employed to create an effective real-time intrusion detection system for general devices. The DCGAN was chosen for its ability to balance positive and negative samples by generating new synthetic data. This model achieved impressive accuracy rates of 99.73% and 99.62% on the KDD and NSL-KDD datasets, respectively, despite limited original data. The area under the curve (AUC) improved from 79.2% to 98% with the augmented dataset. In another study, a GAN was used to classify malware samples by converting them to images for the GAN model. The Mal-IAGAN model demonstrated robustness, achieving over 80% accuracy even when trained on only 1% of a dataset combining Virus Share APK Android malware and the BIG-2015 dataset. This indicates the model's strong generalization capability and effectiveness in handling unseen examples.

Another study model utilizes the NSL-KDD and UNSW-NB15 datasets, along with IoT-23 collected from IoT devices. IoT-23 includes 20 subdatasets from malicious IoT scenarios and three from benign scenarios. The dataset, derived from the Mirai botnet scenario (CTU-IoT-Malware-Capture-34-1), comprises 23,145 IoT network flows categorized into four classes: Benign (normal), C&C (command and control), DDoS, and PortScan (scanning ports for potential attacks).

The study "Generative Adversarial Networks for Cyber Threat Hunting in Ethereum Blockchain" investigates the application of Generative Adversarial Networks (GAN) and Deep Recurrent Neural Networks (RNN), specifically bi-directional Long Short-Term Memory (LSTM), for cyber threat hunting within the Ethereum blockchain ecosystem. Ethereum, known for its decentralized capabilities in Web3 applications, faces vulnerabilities to adversarial attacks.

The proposed model leverages GAN to create synthetic transactions mimicking genuine Ethereum transactions. It then utilizes bi-directional LSTM to distinguish and identify these adversarial transactions from legitimate ones. The findings highlight the model's high accuracy in both generating and detecting adversarial transactions, underscoring its efficacy in enhancing cyber threat detection mechanisms tailored for Ethereum blockchain security.

Supply Chain Management: In supply chain scenarios, ML models monitor goods using IoT sensors to detect tampering or environmental deviations, bolstering security and reliability. Intrusion Detection Systems (IDS) tailored for IoT employ advanced ML approaches for heightened accuracy.

VI. THREAT DETECTION

6.1 Proposed Methods

1. Deep Learning for Intrusion Detection (Otoum et al., 2020): Proposed a DL-oriented intrusion detection framework using the NSL-KDD dataset. Further employed Spider Monkey Optimization (SMO) for feature selection and Stacked Deep Polynomial Network (SDPN) for anomaly detection and achieved an impressive accuracy rate of 99.02%.

2. DL-Oriented Intrusion Detection System (Ge et al., 2020): Utilized the Bot-IoT dataset and a Feed-Forward Neural Network (FNN) for classification of various attacks. Demonstrated high recall, precision, accuracy, and F1 score exceeding 98% across different attack types.

3. Adversarial Attacks on IDS Models (Papadopoulos et al., 2021): Experimented with adversarial attacks (label poisoning and FGSM) on traditional ML and DL IDS models. Highlighted significant impacts on model accuracy and precision under attack scenarios.

4. IoT Intrusion Detection with PSO (Liu et al., 2021): Proposed an IoT intrusion detection model based on Particle Swarm Optimization (PSO) using the UNSW-NB15 dataset. Employed One-Class SVM (OCSVM) for normal and abnormal data recognition. Improved detection rates for various malware types with notable accuracy and reduced false positives.

5. GWO-PSO-RF-NIDS (Keserwani et al., 2021): Introduced an IDS named GWO-PSO-RF-NIDS using a hybrid of Grey Wolf Optimization and Particle Swarm Optimization. Trained and tested on NSL-KDD, KDD Cup99, and CICIDS-2017 datasets. Demonstrated effective intrusion detection capabilities across multiple network environments.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13633

6.2 Generative AI Benefits in Cyber Security

Generative AI offers several "pros" in cybersecurity by enhancing threat detection, response, and defense mechanisms:

[1]. ***Malware Detection:*** Generative AI models trained on large datasets of malware can generate synthetic variants, improving the efficiency of malware detection systems by identifying new patterns and characteristics.

[2]. ***Anomaly Detection:*** Generative AI creates models of normal system behavior, enabling rapid detection of deviations that could indicate security breaches or insider threats.

[3]. ***Password Cracking:*** Using known patterns, Generative AI can generate potential password combinations to strengthen authentication systems.

[4]. ***Threat Intelligence:*** Analyzing vast cybersecurity data, Generative AI generates insights to identify emerging threats and understand attack patterns.

[5]. ***Adversarial AI Defense:*** Generative AI develops defenses against AI-driven attacks, creating synthetic examples to train models against adversarial threats.

[6]. ***Phishing Detection:*** Synthetic phishing emails generated by Generative AI aid in training detection systems and educating users about potential threats.

[7]. ***Network Traffic Analysis:*** By simulating network traffic, Generative AI assists in monitoring and identifying suspicious activities like DDoS attacks.

[8]. ***Automated Security Response:*** Generative AI automates responses to specific threats, deploying countermeasures across networks.

[9]. ***Security Training and Simulation:*** Simulated cyberattack scenarios help security teams practice and refine incident response strategies.

6.3 Cyber Security Issues Using Generative AI

[1]. ***Fundraising:*** Adversaries use ransomware-as-a-service and botnets for financial gain through cryptocurrency mining.

[2]. ***Denial of Service:*** Adversaries use AI to mimic human behavior, launch DDoS attacks, and distribute ransomware emails.

[3]. ***Ransom Emails:*** Generative AI facilitates the creation of ransom demands in multiple languages, aiding cybercriminals.

[4]. ***Malicious Domains:*** AI-generated domains mimic legitimate companies to deceive users.

[5]. ***Phishing Kits:*** AI creates convincing phishing materials, spreading malware to steal personal information.

[6]. ***Manipulated Photos:*** Misuse of AI for morphed photos poses risks, especially impacting investigations.

[7]. ***Fake Digital Content:*** Counterfeit social profiles and synthetic voices deceive users for malicious purposes.

[8]. ***Fake Documents:*** AI fabricates deceptive content, distorting information and compromising intellectual property.

6.4 Mitigating Cyber Security Issues Using Generative AI

[1]. ***Monitoring and Auditing:*** Regular audits of AI systems and collaboration with security teams enhance detection and response capabilities.

[2]. ***AI Security Tools:*** Utilizing AI security tools like Google Cloud Security AI Workbench and Microsoft Security Copilot strengthens defenses.

[3]. ***Secure URLs:*** Understanding URL components and verifying domains mitigate risks of phishing and malicious links.

[4]. ***Public Wi-Fi Security:*** Avoiding automatic connections and using VPNs safeguard against cyber threats in public Wi-Fi environments.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13633

COMPREHENSIVE SURVEY OVERVIEW

Paper	Key Findings	Results	Challenges	Conclusion
Adapting to the AI educational landscape, challenges in Gen AI	Integration challenges in education	Identified barriers and potential solutions	Adoption, training, resources	Strategic approaches for effective AI integration in education
G-ids: Generative adversarial networks assisted IDS	GANs for intrusion detection	Improved detection rates and false positive reduction	Model complexity, training time	GANs enhance IDS effectiveness
Exploring the potential implications of AI-generated content in social engineering attacks	AI's role in social engineering	Potential increase in sophisticated attacks	Detection, prevention, regulation	Need for advanced countermeasures and regulations
A comprehensive survey of generative adversarial networks in cybersecurity intrusion detection	Overview of GAN models in cybersecurity	Identification of strengths and weaknesses	Adversarial attacks, data quality, overfitting	More robust and adaptable GAN models
An enhanced ai-based network intrusion detection system using generative adversarial networks	Novel NIDS using GANs for synthetic data	Improved detection rates and data imbalance handling	Data imbalance, real-time applicability	Improvement of NIDS models, real-world application
Enhancing supply chain insights with Generative AI-driven data analytics and visualization	Generative AI in supply chain analytics	Enhanced insights and visualization	Data accuracy, integration with existing systems	Generative AI can significantly improve supply chain decision-making
Cybersecurity and AI-based threat detection in financial systems	Role of AI in threat detection	Enhanced detection accuracy and response times	Adversarial attacks, data quality, privacy concerns	Explainable AI, federated learning, IoT-specific detection
Cyber sentinel: leveraging AI and ML for advanced threat detection	AI and ML in threat detection	Improved threat detection and mitigation	Data quality, false positives, model robustness	AI and ML are crucial for advanced threat detection
From chatgpt to threatgpt: impact of generative ai in cybersecurity and privacy	Gen AI's impact on cybersecurity and privacy	Identification of new attack vulnerabilities	Privacy, misuse of AI capabilities	Need for security measures/policies
Machine learning techniques for iot security	ML and generative AI in IoT security	Effective threat detection in IoT	Scalability, real-time processing	Generative AI can address IoT security challenges
Synergizing generative artificial intelligence and cybersecurity	Roles of various stakeholders in enhancing cybersecurity with generative AI	Collaborative efforts improve overall cybersecurity	Coordination, data sharing, regulatory compliance	Generative AI requires coordinated efforts from all stakeholders

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024
DOI: 10.17148/IJARCCE.2024.13633

Generative deep learning to detect cyberattacks for the iot-23 dataset	Deep learning for detecting IoT cyberattacks	Improved detection accuracy for IoT-specific attacks	Data diversity, model complexity	Generative deep learning models are effective for IoT cyberattack detection
Unleashing the cyber titans: how AI and ML are shaping future threat detection	Future trends in AI and ML for threat detection	Enhanced threat detection capabilities	Data quality, computational requirements	AI and ML are shaping the future of threat detection
The power of generative AI in cybersecurity: opportunities and challenges.	Opportunities and challenges of generative AI in cybersecurity	New applications and improved threat detection	Adversarial attacks, ethical concerns	Generative AI offers significant opportunities but also poses challenges
Generative adversarial networks for cyber threat hunting in Ethereum blockchain	GANs for threat hunting in blockchain environments	Improved detection of blockchain-specific threats	Data quality, computational complexity	GANs are effective for blockchain threat hunting
Adaptive generative AI for dynamic cybersecurity threat detection in enterprises	Adaptive generative AI for dynamic threat detection	Enhanced adaptability and threat detection	Real-time processing, model adaptability	Generative AI can dynamically enhance enterprise cybersecurity threat detection

Table 6.5 A brief review of survey papers

VII. RESULTS AND EVALUATION

Using Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset: All models were trained on the NSL-KDD dataset and tested on the KDDTest and KDDTest-21 datasets. The highest accuracy was obtained by the CNN1 model on both testing sets, yielding 82.62% and 67.22% accuracy, respectively. An ensemble of all models resulted in accuracies of 86.95% and 76.67% on both testing datasets, respectively. The models involved a hybridization of the Principal Component Analysis (PCA) technique and the Grey wolf optimization metaheuristic algorithm. This approach resulted in a 15% higher accuracy than existing models and a 32% reduction in training time.

Generative Adversarial Networks (GANs) have also been used for data generation and augmentation related to intrusion detection tasks. For example, one study used a GAN to build a sequence of packets from a dataset created using Google Home Mini, generating 42 packets in a sequence with a vocabulary size of 535. The model consisted of an autoencoder and a GAN, where the encoder built the latent space from the sample and sent it to the GAN.

7.1 PROPOSED SOLUTION

Organizations can adapt their defense strategies to mitigate the risks posed by AI-powered social engineering attacks through various approaches:

[1]. ***Tailored Security Advice and Awareness Campaigns:*** Organizations can tailor security advice and awareness campaigns based on the specific needs and expertise of different professional groups to ensure end-user needs are met effectively.

[2]. ***Continuous Improvement of Chatbot Usability:*** Companies developing chatbots for cybersecurity purposes can use feedback from users, such as the System Usability Scale (SUS) questionnaire results, to continually improve the usability of their tools. This can enhance the effectiveness of chatbots in detecting and mitigating AI-driven threats.

[3]. ***Integration of Grounded Theory Analysis into Incident Response Plans:*** Organizations can improve their cybersecurity procedures and incident response plans by utilizing grounded theory analysis derived from qualitative data. Real-world experiences of research participants provide valuable insights on human elements involved in social engineering assaults, which can help in developing more efficient and flexible approaches to address AI-driven risks or threats.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024
DOI: 10.17148/IJARCCE.2024.13633

[4]. ***Creation of Focused Protocols:*** Detailed knowledge of social engineering incidents, including elements like attack context, reasons for falling for attacks, prevention advice, attack strategies, detection methods, and victims' reactions, can guide the creation of focused protocols to handle the unique difficulties presented by AI-generated material in social engineering attempts.

[5]. ***Ongoing Updates and Improvements:*** Organizations should stay informed about the changing landscape of social engineering strategies to inform ongoing updates and improvements to cybersecurity procedures. This proactive approach can help enterprises develop more resilient and adaptable cybersecurity defences against AI-driven threats.

VIII. FUTURE SCOPE

Continuous innovation and technology integration are essential to combat evolving cyber threats effectively. AI systems autonomously identify and analyze cyber threats by continuously learning from data patterns and adapting to evolving threats, enabling organizations to detect and mitigate threats swiftly and accurately, reducing reliance on human intervention. They excel in anomaly detection by analyzing deviations from normal behavior within network traffic and user activities, which helps identify suspicious activities. With advanced algorithms and data-driven insights, these technologies offer unprecedented capabilities in enhancing threat detection and response. Ongoing innovation streamlines incident response processes, automates routine tasks, and optimizes response strategies for faster and more effective mitigation of security incidents. Moreover, innovation and technology integration optimize security operations by leveraging advanced analytics, threat intelligence, and automation capabilities, improving efficiency and resilience. To remain robust against emerging threats, organizations must future-proof their defenses by continuously innovating and integrating adaptable technologies, ensuring long-term cybersecurity success.

IX. CONCLUSION

Integrating IDS with ChatGPT represents a promising advancement in cybersecurity, leveraging AI to enhance real-time threat detection and response capabilities. This innovative approach not only demonstrates the potential of combining natural language processing with security frameworks but also highlights the evolving role of AI in fortifying digital defenses. However, the effectiveness and security implications of such integrations require careful consideration and further research to address potential risks such as model biases and data privacy concerns. Despite these challenges, exploring the synergy between IDS and ChatGPT presents an opportunity for strategies in the future. Using ChatGPT for real-time alerts and LLMs like GPT-4 to protect critical infrastructures also demonstrates how AI is revolutionizing cybersecurity. This survey shows how Next Generation Intrusion Detection Systems (NG-IDSs) are making big strides in dealing with ever-changing cyber threats.

REFERENCES

[1]. Nikolas, Reno & Heng, Ann. (2024). Adapting to the AI Educational Landscape: Challenges of Generative AI Integration. 10.13140/RG.2.2.34893.04320

[2]. M. Shahriar, N. Haque, M. Rahman and M. Alonso, "G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System," in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020 pp. 376-385.

[3]. Al Alahmed, Yazan & Abadla, Reema. (2024). Exploring the Potential Implications of AI-generated Content in Social Engineering Attacks. International Journal of Computing and Digital Systems. 16. 11.

[4]. A. Dunmore, J. Jang-Jaccard, F. Sabrina and J. Kwak, "A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection," in IEEE Access, vol. 11, pp. 76071-76094, 2023, doi: 10.1109/ACCESS.2023.3296707.

[5]. C. Park, J. Lee, Y. Kim, J. -G. Park, H. Kim and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," in IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2330-2345, 1 Feb.1, 2023, doi: 10.1109/JIOT.2022.3211346.

[6]. Stilinski, Dylan & Doris, Lucas & Frank, Louis. (2023). Enhancing Supply Chain Insights with Generative AI-Driven Data Analytics and Visualization.

[7]. Olaoye, Godwin & Williams, Fred (2024) Cybersecurity and AI-based threat detection in financial systems.

[8]. Him, Ibra & Kayode, Sheriffdeen (2023) Cyber Sentinel: Leveraging AI and ML for Advanced Threat Detection.

[9]. M. Gupta, C. Akiri, K. Aryal, E. Parker and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," in IEEE Access, vol. 11, pp. 80218-80245, 2023, doi: 10.1109/ACCESS.2023.3300381

[10]. Alwahedi, Fatima & Aldhaheri, Alyazia & Ferrag, Mohamed Amine & Battah, Ammar & Tihanyi, Norbert. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet of Things and Cyber-Physical Systems. 10.1016/j.iotcps.2023.12.003.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13633

[11]. Jack, Poly & Hurry, Richard. (2024). Advanced Asset Security Management: Leveraging AI and ML for Cyber Threat Detection and Mitigation. 10.13140/RG.2.2.32566.51521.

[12]. Dhoni, Pan. (2023). Synergizing Generative Artificial Intelligence and Cybersecurity: Roles of Generative Artificial Intelligence Entities, Companies, Agencies and Government in Enhancing Cybersecurity. 14. 16. 10.4172/2229-371X.14.3.005.

[13]. N. Abdalgawad, A. Sajun, Y. Kaddoura, I. A. Zualkernan and F. Aloul, "Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset," in IEEE Access, vol. 10, pp. 6430-6441, 2022, doi: 10.1109/ACCESS.2021.3140015.

[14]. Gabbiadini, Alessandro & Ognibene, Dimitri & Baldissarri, Cristina & Manfredi, Anna. (2024). The emotional impact of generative AI: negative emotions and perception of threat. Behaviour and Information Technology. 10.1080/0144929X.2024.2333933.

[15]. S. Sai, U. Yashvardhan, V. Chamola and B. Sikdar, "Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space," in IEEE Access, vol. 12, pp. 53497-53516, 2024, doi: 10.1109/ACCESS.2024.3385107

[16]. Him, Ibra & Kayode, Sheriffdeen. (2024). Unleashing the Cyber Titans: How AI and ML Are Shaping Future Threat Detection

[17]. Wen, Shibo. (2024). The power of generative AI in cybersecurity: Opportunities and challenges. Applied and Computational Engineering. 48. 31-39. 10.54254/2755-2721/48/20241095.

[18]. Shahriar, M.H. et al. (2020) G-ids: Generative Adversarial Networks assisted Intrusion Detection System, arXiv.org. Available at: https://arxiv.org/abs/2006.00676 (Accessed: 13 June 2024).

[19]. Yigit, Y. et al. (2024) Critical Infrastructure Protection: Generative AI, Challenges, and opportunities, arXiv.org. Available at: https://arxiv.org/abs/2405.04874v1 (Accessed: 13 June 2024).

[20]. Lab, E.R.C.S. et al. (2023) Generative adversarial networks for cyber threat hunting in Ethereum blockchain, Distributed Ledger Technologies: Research and Practice. Available at: https://dl.acm.org/doi/10.1145/3584666

[21]. Vemuri, N., Thaneeru, N. and Tatikonda, V.M. (2024) Adaptive Generative AI for Dynamic Cybersecurity Threat Detection In Enterprises, International Journal of Science and Research Archive. Available at: https://ijsra.net/content/adaptive-generative-ai-dynamic-cybersecurity-threat-detection-enterprises