Cyber Threat Detection Using AI

Robert Lourembam
AIT CSE
Chandigarh University
Gharaun ,SAS Nagar Mohali
Punjab (140413)
22bis50001@cuchd.in

Shubham Patel
AIT CSE
Chandigarh University
Gharaun ,SAS Nagar Mohali
Punjab (140413)
22bis50002@cuchd.in

Lalit
AIT CSE
Chandigarh University
Gharaun ,SAS Nagar Mohali
Punjab (140413)
22bis50004@cuchd.in

Neha Sharma
Department of AIT CSE
Chandigarh University
Gharaun ,SAS Nagar Mohali
Punjab (140413)
Neha.e12652@cumail.in

***Abstract*—Within the ever-evolving field of cybersecurity, artificial intelligence (AI) has become a major enabler for threat identification and mitigation. This review examines the various ways that artificial intelligence (AI) might improve cyber defenses. It investigates the incorporation of machine learning algorithms, deep learning frameworks, and AI-driven analytics in swiftly identifying, analyzing, and responding to a variety of cyber threats with unparalleled speed and efficiency. The paper offers a thorough analysis of current AI methodologies, their practical implementations in real-world scenarios, and the challenges encountered in adapting AI to ever-changing threat landscapes. Additionally, it scrutinizes the ethical considerations and potential risks associated with AI's autonomy in decision-making processes. Through synthesizing recent advancements and case studies, this review underscores AI's transformative potential in bolstering cybersecurity measures and shaping the future of digital security infrastructures. The findings underscore the imperative for continuous innovation and collaboration in the field to fully leverage AI's capabilities in combatting cyber threats.**

Keywords—cybersecurity, artificial intelligence, machine learning algorithm, detection, cyber threats, ai-driven analytics

I. INTRODUCTION

The rise of Artificial Intelligence (AI) has transformed the cybersecurity landscape, presenting innovative approaches to combat the constantly evolving challenges posed by cyber threats. This review paper offers a comprehensive analysis of cutting-edge AI techniques leading the way in detecting and mitigating cyber threats. Focusing on recent advancements, we delve into the integration of machine learning, deep learning, and bio-inspired computing across various platforms, including personal computers, cloud services, Android, and the Internet of Things (IoT). Additionally, the paper discusses the dual nature of AI in cybersecurity, recognizing its role in bolstering defenses while also empowering cybercriminals. Through detailed examination of current methodologies and case studies, this paper aims to provide a clear insight into the pivotal role of AI in cybersecurity and its potential to transform the digital threat detection landscape [1].

The rise in cyber-attacks, especially amplified by the widespread adoption of remote work due to the pandemic, has highlighted the urgency for enhanced cyber defense mechanisms. Given AI's prowess in processing extensive datasets and recognizing patterns, it has become an indispensable asset in combating cybercrime. This paper assesses the efficacy of AI-driven tactics in malware detection, network behavior analysis, and real-time incident response. Additionally, ethical considerations and challenges linked to AI's implementation in cybersecurity are deliberated upon, stressing the necessity for a balanced approach that optimizes benefits while mitigating risks.

To conclude, this introduction lays the groundwork for an in-depth examination of AI's transformative influence on cyber threat detection, offering a roadmap for forthcoming research and development endeavors in this vital domain.

II. LITERATURE REVIEW

Sharma et al. (2024) introduced a revolutionary artificial intelligence technique-based cyber threat prediction method. Their suggested Peephole Long Short Term Memory (CbP-LSTM) model, which is based on Cuttlefish, demonstrated exceptional precision and accuracy in detecting cyberthreats. [1].

Saeed and colleagues (2023) carried out a methodical analysis of the literature with an emphasis on Cyber Threat Intelligence (CTI) as a means of enhancing cybersecurity resilience within organizations. They provided a thorough framework that included behavior-based, signature-based, and anomaly-based detection techniques for putting CTI into practice in businesses [2].

This paper offers a comprehensive assessment of the literature on the application of artificial intelligence (AI) techniques to cybersecurity attack detection in Internet of Things (IoT) environments. It places a focus on cutting-edge cybersecurity for IoT solutions and popular AI techniques [3].

This review outlines the state-of-the-art in AI-based malware detection techniques, encompassing Shallow Learning, Deep Learning, and Bio-Inspired Computing methodologies deployed across diverse platforms for malware detection and prevention. [4].

SecurityBERT, a BERT-based model designed for cyber threat detection in Internet of Things networks, was presented by Ferrag et al. This approach revolutionized cyber threat detection in IoT contexts by achieving high accuracy and low inference time, which makes it appropriate for deployment on resource-constrained IoT devices [5].

This study provides an extensive survey with an emphasis on AI-enabled detection of phishing attacks. A comprehensive evaluation of the literature is conducted, encompassing several AI techniques such as Machine Learning, Deep Learning, Hybrid Learning, and Scenario-based approaches [6].

Cyber Security Detection Utilizing Artificial Neural Networks: This AI-based technique for detecting cyber threats leverages artificial neural networks. It transforms security events into individual event profiles, thereby enhancing the detection process. [7].

A review of the application of deep reinforcement learning for threat identification and defense in cybersecurity was carried out by Sewak et al. Their research presented cutting-edge findings in this field [8].

Dash et al. examined the risks and prospects associated with AI-driven intrusion detection systems in cybersecurity, shedding light on the progress and hurdles within this domain. [9].

"Artificial Intelligence in Cybersecurity: Research Advances and Challenges" provides a review of the latest research advancements in AI applied to cybersecurity. The paper also delves into the challenges faced and outlines future directions for AI applications within this domain. [10]

Kalinin M et.el[2023] Detecting security intrusions through the utilization of quantum machine learning techniques.

III. Some traditional method for cyber threat detection

1) **Machine Learning (ML):** Traditional machine learning methods, like Random Forests (RF), Decision Trees (DT), and Support Vector Machines (SVM), are widely used for pattern recognition and cyber threat classification.

2) **Deep Learning (DL):** Convolutional and recurrent neural networks (RNN) in particular are used because of its ability to process sequential data and depict cyberthreats in an image-like format.

3) **Anomaly Detection:**Gaussian Mixture Models (GMM) and k-means clustering are two techniques used to find unusual patterns that may indicate cyberthreats. In order to analyze and understand human language, natural language processing, or NLP, is used. This helps identify phishing and social engineering assaults.

IV. Some newer algorithms for cyber threat detection

1**) Generative Adversarial Networks (GANs):** GANs can be used to generate synthetic cyber threat data, which helps in training robust detection models.

2) **Graph Neural Networks (GNNs):** These are useful for detecting threats in network traffic by modeling the relationships between different entities in a network.

3) **Reinforcement Learning (RL):** RL algorithms can adapt to changing environments, making them suitable for dynamic threat landscapes.

4**) Hybrid Bat Optimization-based Spiking Neural System (BAbSNS):** An architecture integrating the Bat Optimization Algorithm (BAO) and Spiking Neural Network (SNN) for intrusion detection purposes**.**[11]

V. Some mathematical formulation

1)**Support Vector Machine (SVM):** Finding a hyperplane in an N-dimensional space that successfully divides the data points into different classes is the aim of Support Vector Machines (SVM). The decision function can be found using:

$$f(x)=\text{sign}(i=1\sum n\alpha iyi\langle xi,x\rangle+b)$$

The Lagrange multipliers are represented by \(\alpha_i \), the class labels by \(y_i \), the support vectors by \(x_i \), the input by \(x \), the bias by \(b \), and the dot product by \(\langle \cdot, \cdot \rangle \).

2)**Random Forest (RF):** An ensemble of decision trees, wherein each tree casts a vote for a class, and the class receiving the highest number of votes is designated as the model's prediction. The general form of a decision tree can be represented as:

$$f(x)=m=1\sum McmI(x\in Rm)$$

where (M) is the number of trees, (c_m) is the class prediction of the (m)-th tree, (I) is the indicator function, and (R_m) is the region of the (m)-th tree’s decision.

3)**Convolutional Neural Networks (CNN):** Convolution operations are used by Convolutional Neural Networks (CNNs) to analyze data that has a topology resembling a grid. For instance, a 2D convolution in image processing could be used as:

$$S(i,j)=(I*K)(i,j)=m\sum n\sum I(m,n)K(i-m,j-n)$$

In this context, (I) represents the input image, (K) symbolizes the kernel, and (S) indicates the feature map in the main text. Normally, these sections include acknowledgments and references, as demonstrated below. They are formatted without numbering and styled using the "Heading 5" format, similar to "Heading 1" but without enumeration..

VI. Critical analysis

The traditional ML algorithms like SVM, DT, and RF have proven effective in pattern recognition tasks due to their interpretability and ease of use. However, they may struggle with high-dimensional data and require careful feature engineering. DL methods like CNNs and RNNs offer superior performance in processing complex data structures but at the cost of increased computational resources and potential overfitting. Anomaly detection and NLP are crucial for identifying subtle and sophisticated threats, yet they may generate false positives if not finely tuned.

The newer algorithms you’ve mentioned, such as GANs, GNNs, and RL, represent the cutting edge in adaptive and generative models for cyber threat detection. The BAbSNS framework is particularly intriguing as it combines optimization and neural dynamics. However, these advanced methods may face challenges in interpretability and require large datasets for training.

In the 2024 report by the EC Council, they delineated the percentage of AI integration in threat detection [15].

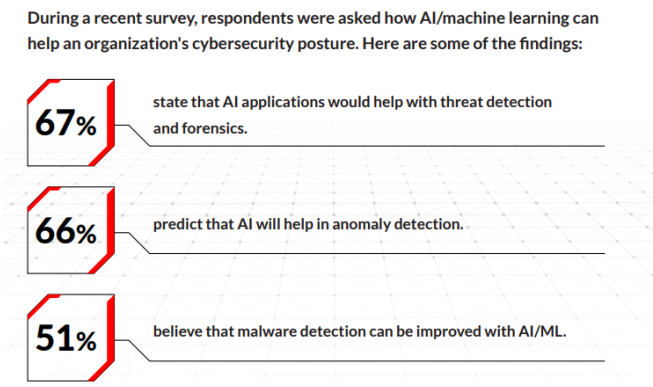

Figure 1

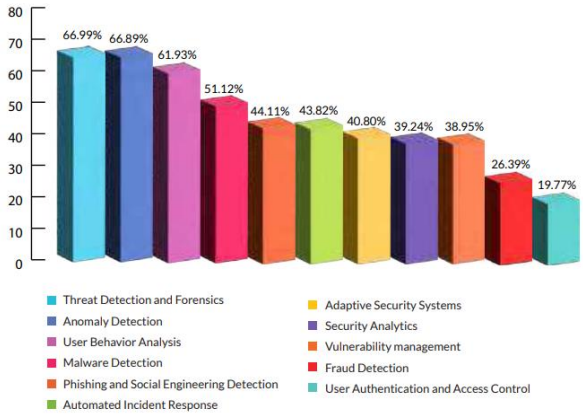

Figure 2

Figure 2 in the report illustrates the specific breakdown of AI utilization across various industries for threat detection purposes.

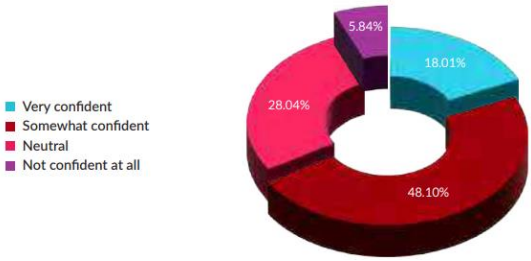

Figure 3

In Figure 3, the report highlights insights regarding the efficacy of AI in combating AI-driven cyber threats. Among respondents, 18% express a strong confidence in AI's ability to aid organizations in defense. Conversely, 49% exhibit moderate confidence, while 27% remain neutral on the matter. Only a minority, constituting 6% of respondents, harbor doubts regarding AI's effectiveness in countering cyber attacks generated by AI systems.

VII. Quantum Machine Learning for Cyber Threat Detection

Quantum Machine Learning (QML) is increasingly recognized as a groundbreaking approach in the realm of cyber threat detection. By merging quantum computing with machine learning techniques, there's potential for the creation of algorithms significantly faster and more efficient than classical methods. This advancement holds promise for devising more effective strategies to identify and counter novel cyber threats.[13]

Researchers investigated the application of Quantum Machine Learning (QML) techniques, such as Quantum Support Vector Machine (QSVM) and Quantum Convolution Neural Network (QCNN), in a paper published in the Journal of Computer Virology and Hacking Techniques. The results showed promising results in terms of high-performance intrusion detection. These techniques have proven to be twice as fast as conventional machine learning algorithms in processing large datasets with astounding accuracy [12].

The World Economic Forum highlights the potential of QML as a new tool in the cybersecurity locker. Stakeholders across academia, industry, and government are showing considerable interest in QML due to its ability to process huge datasets and provide stronger forms of cybersecurity.

Forbes has also reported on the transformative impact of quantum computing on cybersecurity, suggesting that QML may enable more effective algorithms for combating cyberattacks [14].

The results suggest that Quantum Machine Learning (QML) could have a pivotal role in the future of cyber threat detection, presenting a fresh paradigm for safeguarding digital infrastructures against progressively sophisticated attacks. As the domain progresses, it becomes crucial to monitor advancements and assess the impact of quantum technologies on cybersecurity strategies.

VIII. Comparision Table

Study title	Key Points
. Enhancing cyber threat prediction through the implementation of an innovative artificial intelligence methodology.	Presenting a cutting-edge Peephole Long Short Term Memory (CbP-LSTM) model for Cuttlefish that predicts cyber threats with remarkable accuracy and precision.
A comprehensive examination of existing literature on cyber threat intelligence to bolster organizational cybersecurity resilience.	Furnishes an exhaustive framework for incorporating Cyber Threat Intelligence (CTI) within organizations, amalgamating behavior-based, signature-based, and anomaly-based detection methodologies.
Utilizing artificial intelligence methods for the detection of cybersecurity attacks in Internet of Things (IoT) environments.	Examines artificial intelligence methodologies employed for cybersecurity attack detection within the Internet of Things (IoT) domain, emphasizing emerging AI techniques and cutting-edge solutions.
The current advancements in AI-based	Describes AI methodologies utilized in malware detection and prevention, encompassing

techniques for detecting malware.	Shallow Learning, Deep Learning, and Bio-Inspired Computing, deployed across diverse platforms.
A thorough investigation into the detection of phishing attacks enabled by artificial intelligence.	Provides an extensive assessment of the literature on AI approaches, including machine learning, deep learning, hybrid learning, and scenario-based methods, for phishing attack detection.

IX. Research Gap

1)**Integration of AI with Existing Security Frameworks:** While AI techniques are advancing, there is a need for research on how these can be seamlessly integrated with existing cybersecurity frameworks to enhance threat detection without disrupting current operations.

2)**Adversarial AI Attacks:** As AI becomes more sophisticated, so do the methods to exploit it. There is a gap in research on how to defend against adversarial attacks that specifically target AI-based security systems.

Real-Time Processing and Response: Many AI models require significant computational resources, creating a gap in developing lightweight models that can operate in real-time on limited-resource devices, especially in IoT/IIoT environments.

3)**Quantum Resilience:** With the advent of quantum computing, there is a gap in understanding how AI models can be made resilient against quantum attacks and how quantum machine learning can be leveraged for cyber threat detection.

4)**Ethical and Privacy Concerns:** AI systems often process sensitive data, and there is a need for research into models that can detect threats while preserving user privacy and adhering to ethical standards.

5)**AI Explainability**: There is a research gap in making AI decisions more interpretable, especially in critical fields like cybersecurity, where understanding the rationale behind a threat detection is as important as the detection itself.

6)**Behavioral Analysis:** More research is needed on AI systems that can understand and predict human behavior to detect sophisticated social engineering and insider threats.

7)**Standardization and Benchmarking:** There is a lack of standardized benchmarks for evaluating AI-based cyber threat detection systems, which is necessary for comparing different approaches and measuring progress.

8)**Interoperability and Standardization:** There is a need for research on creating interoperable AI systems that can work across different platforms and cybersecurity frameworks to provide a unified threat detection mechanism.

9)**Adaptive AI Models:** Research could focus on developing AI models that can adapt to evolving cyber threats without requiring extensive retraining or manual intervention.

10)**AI Ethics and Governance**: Research into the ethical considerations surrounding the utilization of AI in cybersecurity is imperative, addressing concerns related to privacy, bias, and accountability.

11) **AI and Human Collaboration:** Further research could explore how AI can augment human cybersecurity experts, enhancing decision-making and response times.

12) **Automated Response Systems:** There is a need for research on AI systems that not only detect threats but also autonomously respond to them in a secure and reliable manner.

These identified gaps underscore the necessity for continuous research and development endeavors aimed at tackling the challenges encountered by AI in cyber threat detection. Future studies should strive to bridge these lacunae, ultimately augmenting the effectiveness and dependability of AI in the realm of cybersecurity.

X. Conclusion

In conclusion, a significant development in the realm of cybersecurity is the use of Artificial Intelligence (AI) into the identification of cyber threats. Pattern recognition and classification tasks have their roots in traditional AI models like Random Forests, Decision Trees, and Support Vector Machines. Threat detection has been more precise with the introduction of Deep Learning and its potent Neural Networks, which have further improved the capacity to process and evaluate complicated data structures.

Adaptive and predictive cybersecurity solutions have been made possible by the advent of cutting-edge technologies like Reinforcement Learning, Graph Neural Networks, and Generative Adversarial Networks. These state-of-the-art AI algorithms improve defenses against cyberattacks by not only identifying current risks but also potentially predicting future ones.

Quantum Machine Learning (QML) stands out as a revolutionary approach, promising to redefine the landscape of cyber threat detection. By harnessing the principles of quantum computing, QML offers the potential for exponential improvements in processing speed and efficiency, which are critical in the ever-evolving domain of cyber threats.

With the ongoing rapid evolution of cyber threats, the significance of AI in cybersecurity grows more crucial by the day. The relentless research and development efforts in AI and Quantum Machine Learning (QML) are poised to have a significant impact on shaping a safer digital landscape. It's essential that we remain vigilant and proactive in incorporating these cutting-edge technologies to stay ahead in the ongoing battle against cyber threats.

References

[1] Sharma, P., Prasad, J. S., Shaheen, & Ahamed, S. K. (2024). An efficient cyber threat prediction using a novel artificial intelligence technique.

[2] Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience

[3] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics, 11(2), 1981.

[4] Saeed, S., et al. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience.

[5] Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., Lestable, T., & Thandi, N. S. (2024). Revolutionizing Cyber Threat Detection with Large Language Models: A privacy-preserving BERT-based Lightweight Model for IoT/IIoT Devices.

[6] Ferrag, M. A., et al. (2023). Revolutionizing Cyber Threat Detection with Large Language Models: A privacy-preserving BERT-based Lightweight Model for IoT/IIoT Devices. arXiv preprint arXiv:2306.14263

[7] Harsha, A. Rishika, & Dr. D. Shravani. (2023). CYBER SECURITY DETECTION USING ANN. International Journal of Innovative Engineering, Management & Research.

[8] Sewak, M., Sahay, S. K., & Rathore, H. (2022). Deep Reinforcement Learning for Cybersecurity Threat Detection and Protection: A Review. arXiv preprint arXiv:2206.02733.

[9] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-Based Cyber Security Intrusion Detection: A Review. SSRN Electronic Journal.

[10] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. Artificial Intelligence Review, 55, 1029–1053.

[11] Prince, M. E., Shermila, P. J., Varun, S. S., Devi, E. A., Therese, P. S., Ahilan, A., & Malar, A. J. G. (Year). An optimized deep learning algorithm for cyber-attack detection. Journal Name, Volume(Issue), Page Range. DOI/Publisher.

[12] Kalinin, M., & Krundyshev, V. (2023). Security intrusion detection using quantum machine learning techniques. Journal Name, Volume(Issue), page range. DOI/Publisher

[13] https://link.springer.com/article/10.1007/s11416-022-00435-0

[14] https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/

[15] https://www.eccouncil.org/cybersecurity-exchange/whitepaper/eccouncil-ceh-cybersecurity-threat-report-ai-report/