Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-A, pp. 957–968
DOI : 10.47974/JIOS-1823

Sentinel AI : Pioneering cyber threat detection and mitigation through advanced machine learning

Vandana Agarwal *
Department of Computer Science Engineering
IIMT Engineering College
Meerut 250001
Uttar Pradesh
India

Navnish Goel †
Department of Computer Science Engineering
Dewan VS Institute of Engineering & Technology
Meerut 250103
Uttar Pradesh
India

Manish Sharma §
School of Computer Science & Application
IIMT University
Meerut 250001
Uttar Pradesh
India

Aditya Agarwal ‡
Department of Electronics and Communication Engineering
Faculty of Engineering and Technology
SRM Institute of Science and Technology
Delhi – NCR Campus
Ghaziabad 201204
Uttar Pradesh
India

---

* *E-mail:* **vandanargmeerut@gmail.com (Corresponding Author)**
† *E-mail:* **navnishgoel@gmail.com**
§ *E-mail:* **2k7.manish@gmail.com**
‡ *E-mail:* **aditya.electrobond@gmail.com**

Nisha Gupta [@]
Department of Computer Science
Raghunath Girl's Post Graduate College
Meerut 250001
Uttar Pradesh
India

Sheetal Yadav [#]
Department of Computer Science Engineering
Noida Institute of Engineering and Technology
Noida 201306
Uttar Pradesh
India

Abstract

The Covid-19 pandemic has inevitably caused a sharp increase in the use of digital technologies as only manner of safeguarding ourselves. Covid-19 has forced numerous corporations and companies to adapt to remote work life. Owing to the trends towards digitalization of the key sectors of the economy nowadays, the leading enterprises and schools gradually switch to a remote work. The conclusion on the usage of AI and ML in the cybersecurity system is critical to triumph over the cyber threat and avoiding threats to valuable assets in the developed countries. In this article the author introduces a new product called Sentinel AI that implements machine learning for security purposes. The above system uses both supervised and unsupervised learning techniques which includes the deep learning, anomaly detection as well as the behavioral analysis to detect the known as well as the unknown threats. Since Sentinel AI can learn data patterns consistently, better predictions of threats can be done as well as attempts at faking positive results are slimmer, and hence, it is less susceptible to threats. Next-generation technologies along with the examples of their application and the method of improving the cybersecurity based on the anticipating and preventing threats has also been described in this paper.

Subject Classification: *Primary 68T20, Secondary 68M25.*

Keywords: *Artificial intelligence, Machine learning, Data analysis, Threat detection, Prevention, Cybersecurity frameworks.*

1. Introduction

The unprecedented nature of the coronavirus pandemic has led to the intensification of numerous industries and the ability to introduce artificial

[@] *E-mail:* **gupt.nishu2008@gmail.com**
[#] *E-mail:* **sheetalyadav161@gmail.com**

intelligence (AI), big data. and machine learning (ML) Yet, the current world is evolving at the same pace and has become a place where cybercrime is on the rise threatening usual citizens and well-developed companies. For instance, Eian et al. [1] showing that the prediction of cybercrime could possibly result in a cumulative loss of $10.5 trillion annually by 2025. Consequently, such organizations struggle to manage operation and continuity issues because these technologies have become significantly integrated into business processes. In these lines, there is the need to research on the use of AI in cybersecurity more than ever before. Exploring in this manner would help organizations to realize the whole potential of AI in the field and ultimately foster implementable solutions for safeguarding their operations and interest.

1.1 *Background*

In the realm of cybersecurity, adversaries are persistent, constantly evolving their methods to breach defenses and exploit vulnerabilities. As organizations grew more dependent on digital technologies and distributed work and data, the need to secure that technology has become more acute. More conventional security methodologies, although not useless, are experiencing difficulties in shielding organizations against modern cyber threats. Accompanying the availability, digital security is becoming increasingly vulnerable at the technological frontier of the cyberspace, which in turn emphasizes the importance of tools to identify cyber threats effectively [2]. Today's complex and dynamic cyber threats pose threats to organizational security, and the complex nature of these risks has exposed the weakness of traditional security models in dealing with them [3]. Holding security from cyber threat has become more essential in today's world since the interaction in electronic interface increases and the elaboration of malicious attacks become more complex. This research is about illustrating the use, advantage, approach, and real-world utilization to revolutionary cyber threat identification and defense by using sophisticated artificial intelligence techniques

2. Literature Review

Kumar et al., [4] opine that AI and ML can be employed as tools that are of revolutionary nature in addressing constantly evolving nature of cyber threats. Through real time identification and mitigation of threats, these technologies are capable of transforming the business of security

and increase current methods. Traditional and passive approaches of security are no longer adequate in combating the modern and adaptive nature of cybersecurity threats [5-9]. Threats are dynamic; they change with time, making it all the more important to have a constant cybersecurity measure. For this reason, as was previously mentioned in the case of offense, the defenses must also be active and continuous. Summarized literature about AI application in the catching of threats in the field of cybersecurity is presented in Table 1.

Table 1
Artificial Intelligence (AI) in medical diagnosis

References	AI Domain	Key Finding
M. Nasser et. al. [10]	Yes	The authors analyzed cases as well as incidents in cyber-physical systems through writing a variety of security breaches as well as offered ways through which such breaches should be controlled.
Hariharan et. al. [11]	Yes	The researcher likely concludes by emphasizing the significance of explainable artificial intelligence (XAI) in enhancing transparency and trustworthiness within cybersecurity practices.
Lallie et. al. [12]	No	The authors highlight the way of cyber-attacks after the Covid-19 pandemic and their possible solutions.
Mishra et. al. [13]	Yes	The authors propose a Binary Grasshopper Optimized Twin Support Vector Machine (BGOTSVM) supported security model. Learning-based models for network intrusion detection utilizing ML techniques.
Farouk et. al. [14]	Yes	The authors identified ML classifier for detecting internal threats specifically to secure LAN attacks.
Singh et. al. [15]	Yes	To detect malware the authors utilized Feed - Forward Deep Neural Network (FFDNN) technique.
Li [16]	Yes	The authors elaborate on the existing research on building a secure AI system in distributed ML/DL surroundings using encrypted neural network as well as realizing a secure federated deep learning.

Contd...

Ghillani [17]	Yes	The goal is to discuss the numerous ways in which deep learning techniques and neural network architectures might be used to provide cybersecurity solutions. They conclude that the advanced learning algorithms need to be trained using the obtained security data and knowledge related to the intended application before the system can assist in making intelligent decisions.
Islam, Hayat, and Hossain [18]	Yes	The authors focus on the right mix between AI's advantages and human abilities to optimize its benefits and minimize its disadvantages. The study makes recommendations for future research to address fresh issues pertaining to the efficient use of AI in cyber security.

3. AI-Based Threat Detection Techniques

Artificial intelligence (AI) refers to perform a task by computer systems that typically require human intellect. Within cybersecurity, AI mimics human cognitive procedures learning, reasoning, problem-solving, and decision-making for such tasks. It has become increasingly important in this field, on account of its capacity to process large volumes of data in relatively short time and arrive at sound decision-making, all-in light of new forms of cyber threats. With the volume and complexity of these threats continue to rise, organizations are accepting AI-based systems for detecting and preventing cyber-attacks. These systems utilize techniques such as ML, Natural Language Processing (NLP), DL, Natural

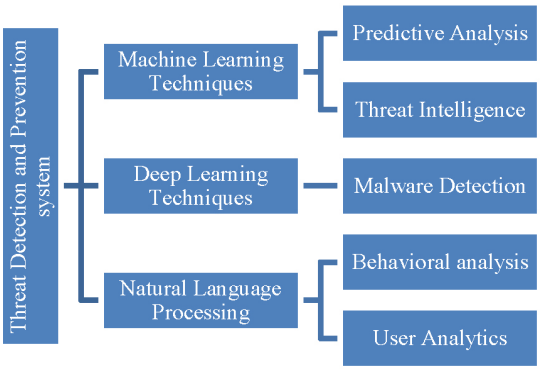

Figure 1

Comprehensive Framework of AI-Based Threat Detection in Cybersecurity

Language Processing (NLP), predictive analytics, and behavioral analytics, as showed in Figure 1, to detect and mitigate cyber threats effectively [19].

3.1 *Fraud Detection Systems Using AI*

Application for threat detection is an AI whereby threat detection compares a large dataset and automatically identify security threats. By using mandate learning algorithms, these systems are able to first recognize anomalous traffic patterns, second to recognize the presence of virus in separated files, and third to analyze user activity for possible malicious activity [20]. In the financial industry, fully automated artificial intelligent-based fraud detection mechanisms scan through large volumes of data to identify fraudulent transactions based on anomalous patterns and trends within financial transactions [21]. Machine learning threat intelligence solution uses real-time data collection over various sources and researches growing threats and risks. In the case of incident response, AI based systems enhance the preparedness and time taken in managing cyber threats as they rapidly analyze different data formats and provide remedial advice to the security teams [22]. Furthermore, traditional security tasks like bookings, account creation and password changes are performed automatically by intelligent chatbots and virtual assistants. These are not just effective in simplifying work processes however they also give instant assistance to its users effectively improving security response factors.

3.2 *Fraud Detection Systems Using ML*

AI solutions improve the cybersecurity postures by providing the means for counteraction to change continuously about threats. Namely, artificial intelligence with machine learning in particular, as a discipline which aims at creating a system for recognizing pattern in data and drawing conclusions without a direct programming step, is important. Conventional security solutions were mostly based on a signature or set of signatures of known threats; a model becoming less efficient to prevent modern and evolved cyberattacks. On the other hand, AI solutions use multiple intricate mathematics formulas and machine intelligence technique for identifying existing and new hazardous elements. Machine learning, widely used in threat detection [23], deals with the large volume of data where the likely patterns of threats are also identified. Due to the fact that these algorithms are adapted to take data subsets that contain vice and non-vice activities, they are in the best position to identify

network behavior anomalies that may signal the likelihood of a security breach.

3.3 *Fraud Detection Systems Using Deep Learning*

Deep learning models use deep neural networks to classify data and break down data into categories where certain elements of the data may be assigned binary economic classifications. In fraud detection, Neural Networks can be also used for predicting fraudulent transactions from big data sets of transaction records. Indeed, the models can be used as deep neural networks, that is, they can have multiple layers that can learn representations of growing complexity. Neural Networks also has the ability to analyze any form of data input, whether numeric and categorized like transactions, pattern or textual. Recurrent Neural Network (RNN) and convolutional Neural Network (CNN) are the kind of neural networks analyze sequences of events in order to ascertain patterns that may point towards forged documents.

3.4 *Fraud Detection Systems Using Hybrid Model*

In order to combine advantages of both methods, in the hybrid models the methods of supervised and unsupervised machine learning methodologies are used [24-25]. Supervised learning utilizes input datasets for training purposes while unsupervised learning identifies patterns without predefined input. Hybrid techniques [26] aim to enhance accuracy by combining the precision of supervised and unsupervised learning. Boosting and bagging techniques [27] merge outputs from multiple models to mitigate individual model limitations. The use of ensemble learning which increases the accuracy on threat prediction is especially effective when used in real-time cybersecurity applications. Cyber threat clustering is helpful to know anomaly detection and organizing related threats [28].

4. Fraud Detection Systems Using the Proposed Modified Hybrid Model

This paper argues that fraud detection systems play a significant role in the protection of financial transactions together with minimizing the increasing cases of fraud. This work addresses the efficacy of a newly developed approach for enhancing the skills in fraud detection through the application of a Modified Hybrid Model with Generative AI hallucinations to detect fraudulent behavior.

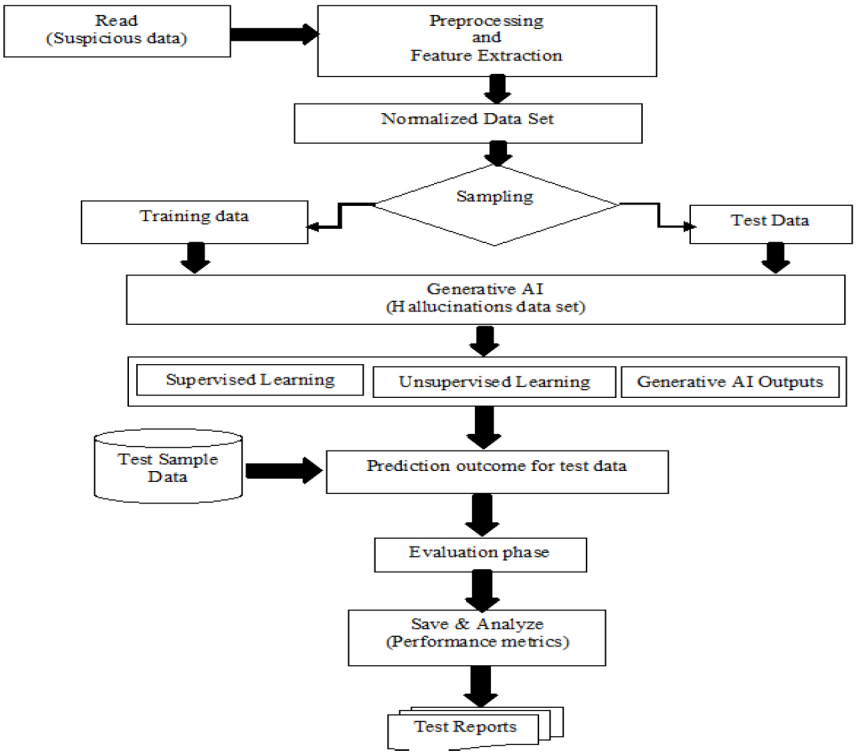

Figure 2

Work Flow diagram of FDS using Hybrid Model with Generative AI Hallucinations

How it Works

The Modified Hybrid Model incorporating Generative AI hallucinations for fraud detection is also used where different ML methods integrate to increase detection accuracy and speed. Here's how it operates in Figure 2.

5. Discussion and Conclusion

Since threats can be delivered in a variety of methods, there is no fixed strategy for protecting against them. It is important to identify that recent reviews show that IDSs based on AI algorithms provide higher reliability and better adaptivity than traditional IDSs. They are dynamic in that new model real-life data can be used to enhance the existing systems making them relevant to emerging cyber threats. Real-time threat data

integration improves their capability on integrational perception of current threats and events, and real-time prediction systems change with the last tactics and methods of adversaries. This paper therefore emphasizes on the importance of ML and AI in enhancing cybersecurity against an ever-growing number of threats. It stresses for the approaches to the integration with other fields, continuous improvement, and changes in the strategies in order to respond to the current situation in the field of cybersecurity. However, it remains imperative to remember that the given AI should be people-centered, so it must have human values & considerations. However, there are potential and real AI-based issues; therefore, AI is promising to strengthen cybersecurity for the continually growing society.

Reference

[1] I. C. Eian, L. K. Yong, M. Y. X. Li, Y. H. Qi, and F. Z, "Cyber Attacks in the Era of COVID-19 and Possible Solution Domains," *www.preprints.org* (Sep. 2020), doi:https://doi.org/10.20944/preprints202009.0630.v1.

[2] Yusuf Yusuf Dayyabu, D. Arumugam, and Suresh Balasingam, "The application of artificial intelligence techniques in credit card fraud detection: a quantitative study," *The application of artificial intelligence techniques in credit card fraud detection: a quantitative study*, vol. 389, pp. 07023–07023 (Jan. 2023), doi:https://doi.org/10.1051/e3sconf/202338907023.

[3] C. Obi, V. Akagha, S. Onimisi, A. Chigozie, N. S. Onwusinkwue, and A. Ibrahim, "Comprehensive review on cybersecurity: modern threats and advanced defense strategies," *Computer science & IT research journal*, vol. 5, no. 2, pp. 293–310 (Feb. 2024), doi:https://doi.org/10.51594/csitrj.v5i2.758.

[4] S. Kumar, U. Gupta, A. Singh, and A. K. Singh, "Artificial Intelligence," *Journal of Computers Mechanical and Management*, vol. 2, no. 3, pp. 31–42 (Aug. 2023), doi:https://doi.org/10.57159/gadl.jcmm.2.3.23064.

[5] M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Computers & Security*, vol. 88, p. 101636 (Jan. 2020), doi:https://doi.org/10.1016/j.cose.2019.101636.

[6] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, no. 3, pp. 395–411 (May 2018), doi:https://doi.org/10.1016/j.future.2017.11.022.

[7] M. Rege, R. Blanch, and K. Mbah, "Machine Learning for Cyber Defense and Attack.https://personales.upv.es/thinkmind/dl/conferences/dataanalytics/data_analytics_2018/data_analytics_2018_5_30_60121.pdf.

[8] M. Chowdhury, A. Rahman, and R. Islam, "Malware Analysis and Detection Using Data Mining and Machine Learning Classification," *Advances in Intelligent Systems and Computing*, pp. 266–274 (Oct. 2017), doi:https://doi.org/10.1007/978-3-319-67071-3_33.

[9] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, no. 101804, pp. 1–29 (2023), doi:https://doi.org/10.1016/j.inffus.2023.101804.

[10] Mohammed Nasser Al-Mhiqani, Rabiah Ahmad, Warusia Yassin, Aslinda Hassan, Zaheera Zainal Abidin, Nabeel Salih Ali and Karrar Hameed Abdulkareem, "Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems" *International Journal of Advanced Computer Science and Applications*(ijacsa), 9(1) (2018).

[11] S. Hariharan, A. Velicheti, A. S. Anagha, C. Thomas, and N. Balakrishnan, "Explainable Artificial Intelligence in Cybersecurity: A Brief Review," *IEEE Xplore*, Oct. 01 (2021). doi:https://doi.org/10.1109/ISEA-ISAP54304.2021.9689765.

[12] Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput Secur. 2021 Jun; 105 : 102248. doi: 10.1016/j.cose.2021.102248. Epub 2021 Mar 3. PMID: 36540648; PMCID: PMC9755115. https://pmc.ncbi.nlm.nih.gov/articles/PMC9755115/

[13] R. Mishra, "Cyber Security Threat Detection Model Using Artificial Intelligence Technology," (Jul. 2023). doi:https://doi.org/10.1109/icecaa58104.2023.10212209.

[14] M. Farouk, R. H. Sakr, and Noha Hikal, "Identifying the most accurate machine learning classification technique to detect network threats," *Neural Computing and Applications*, vol. 36, no. 16, pp. 8977–8994 (Mar. 2024), doi:https://doi.org/10.1007/s00521-024-09562-9.

[15] P. Singh, S. K. Borgohain, A. K. Sarkar, J. Kumar, and L. D. Sharma, "Feed-Forward Deep Neural Network (FFDNN)-Based Deep Features for Static Malware Detection," *International Journal of Intelligent Systems*, vol. 2023, pp. 1–20 (Feb. 2023), doi:https://doi.org/10.1155/2023/9544481.

[16] J. Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474 (Dec. 2018), doi: https://doi.org/10.1631/fitee.1800573.

[17] Diptiban Ghillani, "Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security," (Sep. 2022), doi: https://doi.org/10.22541/au.166379475.54266021/v1.

[18] S. Islam, M. A. Hayat, and M. F. Hossain, "Artificial intelligence for cybersecurity: impact, limitations and future research directions," Dec. 27 (2023). doi: https://doi.org/10.5281/zenodo.10448268.

[19] G. Rekha, S. Malik, A. K. Tyagi, and M. M. Nair, "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 3, pp. 72–81 (2020), doi: https://doi.org/10.25046/aj050310

[20] Tariq Bishtawi and Reem Alzubi, "Cyber Security of Mobile Applications Using Artificial Intelligence," (Nov. 2022), doi:https://doi.org/10.1109/eiceeai56378.2022.10050484.

[21] M. Marripudugala, "AI-Powered Fraud Detection in the Financial Services Sector: A Machine Learning Approach," *2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, pp. 795–799 (Oct. 2024), doi: https://doi.org/10.1109/icssas64001.2024.10760599

[22] K. R. Bhatele, H. Shrivastava, and N. Kumari, "The Role of Artificial Intelligence in Cyber Security," *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems*, pp. 170–192 (2019), doi: https://doi.org/10.4018/978-1-5225-8241-0.ch009.

[23] E.-C. University, "Machine Learning in Cybersecurity: How it Works and What Companies Need to Know," *Accredited Online Cyber Security Degree Programs | EC-Council University*, Oct. 12 (2023). https://www.eccu.edu/blog/cybersecurity/machine-learning-in-cybersecurity/.

[24] E. Oye, P. Peace, and J. Owen, "The Role of Natural Language Processing in Cybersecurity," *ResearchGate*, Dec. 20 (2024). https://www.researchgate.net/publication/387252722_The_Role_of_Natural_Language_Processing_in_Cybersecurity.

[25] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," *Applied Sciences*, vol. 9, no. 20, p. 4396 (Oct. 2019), doi:https://doi.org/10.3390/app9204396.

[26] S Senthil Pandi, M.S. Monesh, and B. Lingesh, "A Novel Approach to Detect Face Fraud Detection Using Artificial Intelligence," pp. 1–6 (Feb. 2024), doi: https://doi.org/10.1109/ic-etite58242.2024.10493594.

[27] M. Kalirane, "Ensemble Learning Methods: Bagging, Boosting and Stacking," *Analytics Vidhya*, Jan. 20 (2023). https://www.analyticsvidhya.com/blog/2023/01/ensemble-learning-methods-bagging-boosting-and-stacking/.

[28] Mahmoud Mahfuri, Sameh Ghwanmeh, Rsha Almajed, Waseem Alhasan, Mohammed Salahat, and Jin Hie Lee, "*Transforming Cybersecurity in the Digital Era: The Power of AI*," (Feb. 2024), doi: https://doi.org/10.1109/iccr61006.2024.10533072.

Received October, 2024