ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

Examine The Role Of Generative AI In Enhancing Threat Intelligence And Cyber Security Measures

[1]Dadi Sahithi, [2]M.Radhika

[1]Student, Dept of CSE, MAM women's engineering college, Kesanupalli, narasaraopet.
[2]Professor, Dept of CSE, MAM women's engineering college, Kesanupalli, narasaraopet.

Abstract

Organizations are using generative artificial intelligence (AI) more and more to improve their cyber security and threat intelligence. AI that generates new data without depending on preexisting data or expert knowledge is known as generative AI. By considering several sources and data points, this technology enables decision support systems to automatically and swiftly identify threats posed by hackers or hostile actors. Furthermore, generative AI can assist in locating weak points in an organization's infrastructure, which lowers the likelihood that an assault would succeed. For security operations centers (SOCs), which need to quickly identify threats and take preventative action, this technology is particularly well-suited. Generative AI can give businesses an extra line of defense against increasingly complex threats by integrating intriguing and useful data items that would have otherwise gone unnoticed.

Keywords: Cybersecurity, Threat Intelligence, Generative AI, Improving, and Measures

I. INTRODUCTION

In recent years, artificial intelligence, or generative AI, has become a vital tool in the field of cyber security and threat intelligence [1]. AI provides an automated and advanced way to find network, system, and application vulnerabilities that could lead to a cyberattack [2]. These artificial intelligence (AI) technologies can identify hidden threats before they lead to an assault, giving companies ample time to take the appropriate safety measures. Generative AI is based on predictive analytics, which enables it to recognize potential threats such as malicious URLs or other malware [3]. It can also identify suspicious or odd user activity and insider threats. With the use of advanced analytics, AI can effectively detect such hazards before they materialize. Another benefit of using generative AI to enhance threat intelligence and cyber security measures is its ability to automate threat analysis [4]. By continuously evaluating enormous data sets that track the functioning of networks and systems, AI may detect any suspicious activity without the help of humans [5]. As a result, the efficiency of theprocedure, as well as the precision of the information gathered and the degree of threat identification. A growing topic is the application of generative AI to improve cyber security and threat intelligence [6]. The efficacy and precision of threat detection and response strategies could be significantly increased by this technology. Businesses have the visibility they need to identify threats early on and take action to lessen the effect of any resulting damages thanks to AI-driven threat intelligence and cyber security measures [7]. One kind of artificial intelligence (AI) that can learn on its own and acquire new skills is called generative AI. It is distinguished by the capacity to examine vast amounts of data, spot trends, spot irregularities, and create plans to strengthen an organization's security. With the help of generative AI, an organization may gain more detailed insight into its surroundings, enabling better security protocols and a better comprehension of the hazards present in the always changing digital scene. The firm can take proactive steps to prevent damage by using generative AI to uncover hazards that might otherwise go unnoticed [8]. Additionally, it has the ability to identify common risks including network breaches, malicious material, and phishing attempts. The following figure 1 displays the building diagram.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

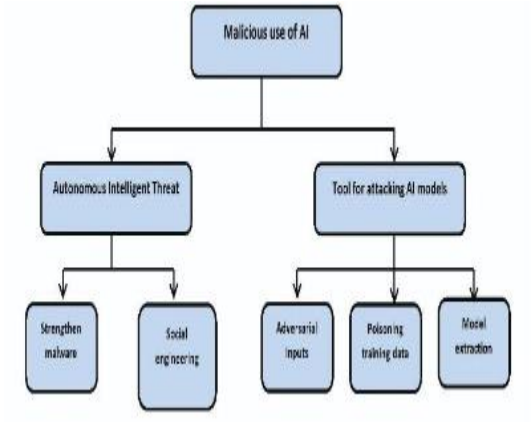

Fig. 1. Construction diagram

When malevolent individuals are identified, this AI can produce alarms by analyzing the system's behavior patterns [9]. This gives enterprises more insight into their surroundings and enables them to take precautions against possible threats. This paper's primary contribution is as follows:

1. Automation of threat intelligence and cyber security processes: Generative AI enables automated threat intelligence gathering and updating of cyber security measures, eliminating manual labor and allowing for complex and sophisticated risk analysis of potential threats. 2. Improved detection and mitigation of malicious activity: Through the use of generative AI, organizations can gain greater insight into which attack vectors are more likely to be used, and respond accordingly by finding the most effective methods to detect and neutralize the threat. 3. Increased efficiency in threat analysis: By utilizing generative AI, organizations can quickly analyze large amounts of threat data and extract useful insights for further protection. This increases efficiency in threat analysis and leads to better informed threat-based decisions. 4. Improved network monitoring: Generative AI provides enhanced network monitoring capabilities, enabling organizations to continually scan networks and identify anomalous activities, and accordingly take preventive measures to protect against cyberthreats. 5. Advanced AI-driven threat intelligence: Generative AI can be used to generate AI-driven threat intelligence, allowing for deeper insight into potential threats and better security decisions.

II. RELATED WORKS

As businesses seek to improve their threat intelligence and cyber security protocols, generative artificial intelligence (AI) has grown in significance in recent years [10]. The process of producing new and frequently inventive data is known as "generative AI," and it uses algorithms made to learn from preexisting information and produce previously unimagined concepts. In the field of cybersecurity, generative AI can assist companies in recognizing emerging risks, creating defences against them, and promptly and effectively responding to existing ones [11]. The first way that generative AI may support cyber security operations is by offering a comprehensive understanding of the threat landscape facing a business. It can examine existing datasets to find patterns that haven't been found before, detect possible dangers, and make specialists more aware of potential weaknesses [12]. Generative AI may also assist companies in anticipating and addressing new risks by offering insights into the fundamental patterns and actions of malevolent actors. Additionally, generative AI can assist cyber security professionals in creating and implementing more effective preventative measures. Experts can use threat activity data to find previously unnoticed patterns and use that information to create stronger countermeasures [13]. Additionally, generative AI can handle the workload of evaluating a high volume of threat intelligence feeds, freeing up human experts to concentrate on those that need further study and analysis. Last but not least, generative AI may automate processes like obtaining information about specific hazards, sending out alerts, building dashboards, and connecting data points to support investigations. Threat intelligence and cyber security protocols could be completely transformed by generative artificial intelligence, or generative AI [14]. A kind of machine learning known as "generative AI" allows computers to create or synthesis new data sets from pre-existing ones, improving and increasing the precision of data-driven decision making [15]. Through the incorporation of generative AI into theData breaches, malware attacks, and other harmful behaviour can be prevented and detected by improving cyber security procedures, threat intelligence, and cyber security systems. Large amounts of data gathered from security systems, such as network traffic, user activity, and content, can be used by generative AI to create and implement unique risk-based formulae that swiftly identify hostile activity [16]. Additionally, generative AI may assess an organization's security posture, investigate its network, and notify cyber security experts of any questionable activities. Furthermore, generative AI can identify unusual patterns and behaviours and develop fresh approaches to thwart dangers. Additionally, by incorporating machine learning models into the organizational security infrastructure, generative AI can offer a higher level of data protection. These models have the

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

ability to recognize threats and notify cyber security experts of possible dangers. Finding the best answer to the aforementioned issues is the primary originality of this study. These include the potential for generative AI to significantly enhance threat intelligence and cyber security protocols [17]. Without assistance from humans, generative AI models may create new data by learning from examples. This could assist organizations in identifying hidden or invisible risks and their trends. Additionally, big datasets collected from many sources can be swiftly analysed by AI-enabled systems, which can identify dangers almost instantly. Furthermore, organizations might create complex fake data intended to snare potential attackers with the aid of generative AI models. This data can assist lower the danger of data disclosure during an assault because it is automatically generated and can be used to conceal the actual data.

III. PROPOSED MODEL

An upcoming technology called generative artificial intelligence, or generative AI, has the potential to completely transform cyber security and threat intelligence procedures. The development of more effective solutions that lower the expense and complexity of threat intelligence and cyber security measures may be made possible by generative AI. Deep learning techniques are used by generative AI to find and examine patterns and connections in data. By leveraging the processing power of the computer, generate AI can detect anomalies and identify
security threats faster than manual approaches. Because AI can precisely detect high-risk scenarios and notify the user, this enables the implementation of more effective and efficient security measures. Furthermore, the performance and effectiveness of security systems can be tested and assessed by using generative AI to create simulations of real-world situations. Among other things, these simulations can mimic situations like a hacker attack, harmful software, or dangerous network behaviour. Businesses can make sure they have the appropriate amount of cyber security measures in place by evaluating the security measures' efficacy before implementing them.

$$p''(o) = \lim_{o \to 0} \left(\frac{p(p+o) - p(o)}{o} \right) \qquad (1)$$

$$p'(o) = \lim_{p \to 0} \left(\frac{p^{p+o} - p^{p}}{o} \right) \qquad (2)$$

A new area of artificial intelligence called "generative AI" allows computers to produce original concepts and results. Deep learning is one example of generative AI technology.To improve cyber security measures, more complex threat intelligence models can be produced using architectures and generative adversarial networks (GANs). By facilitating the creation of increasingly complex models, generative AI contributes to the expansion of threat intelligence capabilities. A GAN, for instance, can be used to create malware, phishing campaigns, new dangerous code, and other harmful actions. Furthermore, more intricate attack networks that are able to recognize network patterns can be developed using generative AI.

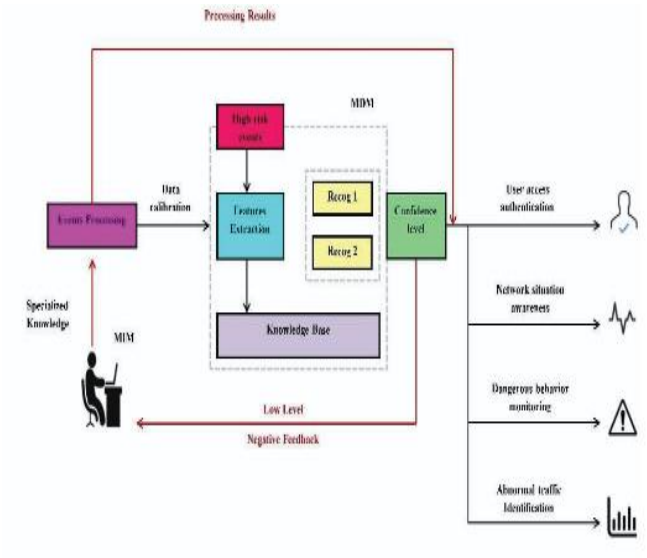

Fig. 2. Functional block diagram

One type of artificial intelligence that can be used to generate or create new data is called generative AI. Its primary uses are in the fields of cyber security and threat intelligence. The way generative AI operates is by combining information from both structured and unstructured parameters, user feedback, and a variety of internal and external sources.

$$p(o) = \lim_{p \to 0} \left(\frac{(p^{p} * p^{o}) - p^{p}}{o} \right) \qquad (3)$$

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

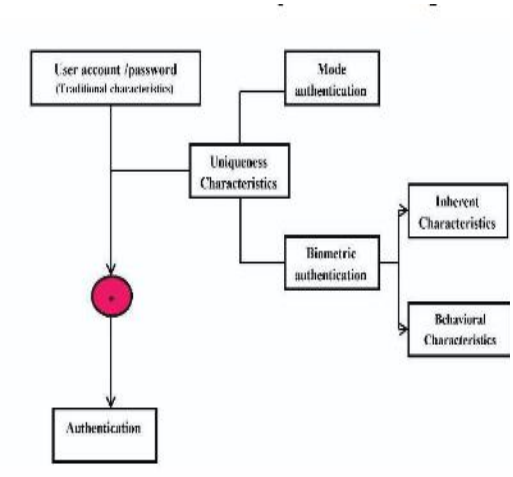

Fig. 3. Operational flow diagram

An artificial intelligence (AI) technology called generative AI is used to create new, never-before-seen data or data that appears unique or real. Using probability models, generative AI creates data or information according to a set of parameters and conditions. Threat intelligence and strengthening cyber security measures are just two uses for this data.

$$p(o) = e^{p} * \lim_{p \to 0} \left(\frac{1 - e^{p}}{o} \right) \quad (5)$$

$$\partial o = \partial e^{p} - 1 \quad (6)$$

$$\partial p^{o} = \partial o + 1 \quad (7)$$

$$\partial p = \ln(o + 1) \quad (8)$$

Existing cyber security solutions can be informed and safeguarded by using the new threat intelligence generated by generative AI.

IV. RESULTS AND DISCUSSION

A new type of AI technology that is becoming more and more common in cyber security is called generative artificial intelligence (AI). Organizations can better defend their networks and systems against malevolent actors thanks to generative AI's increased automation and quicker threat identification. BERT (Bidirectional Encoder Representations from Transformers), WGAN (Wasserstein Generative Adversarial Network), SPADE (Spatially Adaptive Denormalization), and DCGAN (Deep Convolutional Generative Adversarial Network) have all been compared to the suggested model.

A. Evaluation of Accuracy

Using data from many sources, generative AI adopts a more comprehensive approach to security by producing a real-time picture of dangers and their ability to wreak havoc. The automation of threat detection enables firms to react to potential attacks more rapidly and effectively. Table 1 presents an accuracy comparison of different algorithms.

TABLE I. COMPARISON OF ACCURACY (IN %)

No.of rounds	DCGAN	WGAN	BERT	SPADE	Proposed
200	85.90	82.24	66.77	80.44	88.30
400	86.87	83.24	68.37	82.28	89.08
600	87.51	83.79	73.16	83.16	89.70
800	88.55	85.64	74.17	83.83	90.97
1000	89.87	86.02	75.46	84.87	92.28

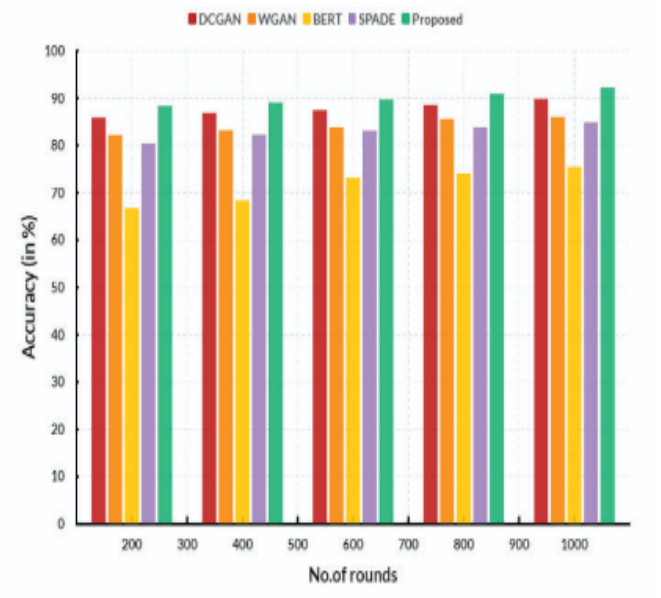

Fig. 4. Comparison of Accuracy

Furthermore, because generative AI can recognize behaviours that can point to harmful conduct, it enables enterprises to proactively identify dangers before they materialize. Instead of only passively monitoring their networks, this solution enables firms to take a more proactive approach to cyber security. It is possible to perform a performance analysis of generative AI to ascertain how well it enhances an organization's security and threat intelligence protocols. Assessing elements like

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

detection latency, accuracy, scalability, and customizability can help achieve this. An organization can identify risks more quickly if its detection latency is shorter.

B. Evaluation of False positive rate

Instead of merely converting current data into potentially useful forms, generative AI uses AI to produce new, distinct, and useful data from existing data. Generative AI is playing a significant part in the creation of better threat intelligence solutions and is becoming more and more significant in strengthening cyber security measures. Realistic threat models produced by generative AI can be used to analyse and appraise possible security threats. Multiple virtual simulations of real-world hazards can be produced by generative AI models using extensive data sets. A comparison of different algorithms for the false positive rate is provided in Table 2.

TABLE II. COMPARISON OF FALSE POSITIVE RATE (IN %)

No.of rounds	DCGAN	WGAN	BERT	SPADE	Proposed
200	81.90	78.24	62.77	77.44	83.30
400	82.87	79.24	64.37	79.28	84.08
600	83.51	79.79	69.16	80.16	84.70
800	84.55	81.64	70.17	80.83	85.97
1000	85.87	82.02	71.46	81.87	87.28

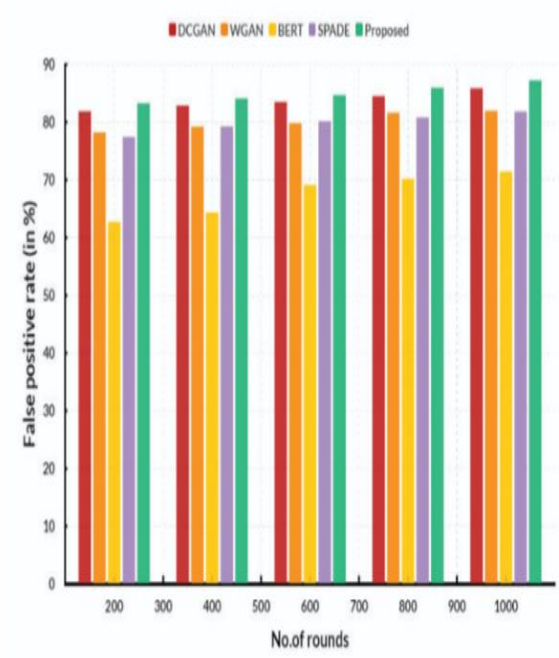

Fig.5: Comparison of false positive rate

To create effective countermeasures, these simulations can be used to learn from a variety of circumstances. In order to find and examine vast amounts of both organized and unstructured data, generative AI can also be used to spot possible unusual activity, such hostile activity. In order to identify patterns and abnormalities in data that would be hard or impossible to find with conventional security solutions, generative AI models imitate human behaviour. This may result in enhanced threat identification, enablingorganizations to successfully address risks before they worsen.

C. Evaluation of False negative rate

The application of AI and machine learning to cyber security and threat intelligence is growing in popularity. AI is shown itself to be a useful tool for assisting in the detection and prevention of malicious activity as threats continue to grow more sophisticated. In particular, generative AI is being applied in a variety of ways to improve security protocols.

Real-time danger detection is possible with generative AI. Table 3 compares several algorithms for the false negative rate.

Table.3. Comparison of false negative rate (in %)

No.of rounds	DCGAN	WGAN	BERT	SPADE	Proposed
200	84.90	81.24	65.77	81.44	87.30
400	85.87	82.24	67.37	83.28	88.08
600	86.51	82.79	72.16	84.16	88.70
800	87.55	84.64	73.17	84.83	89.97
1000	88.87	85.02	74.46	85.87	91.28

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 16, Issue 3, 2025

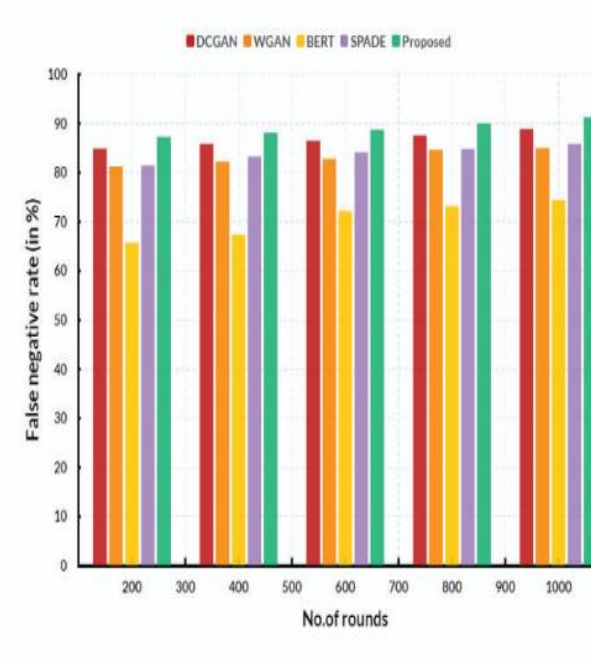

Fig. 6. Comparison of false negative rate

This aids in identifying harmful activities that conventional security systems could overlook. It can also be used to examine user behaviour on different platforms and find trends that can point to a breach or malicious conduct. In order to create better secure systems, generative AI can also be used to create "what-if" scenarios or simulations that mimic a possible attack and the harm it could cause. In order to save time and money on maintaining secure systems, generative AI can also be utilized to automate security procedures. AI can also be used to spot and draw attention to questionable activities that people might overlook. Lastly, to keep ahead of possible threats, security systems can be continuously monitored and updated using generative AI.

D. Evaluation of Response time

Artificial intelligence that can automatically learn from datasets to produce new, previously unseen data is known as generative AI. By identifying risks before they become harmful or hazardous, it can be utilized to enhance threat intelligence and cyber security procedures. Generative AI can be used to quickly spot data irregularities and notify security staff of potential threats. Better overall defense against cyberattacks and quicker reaction times may result from this. Table 4 compares several algorithms for reaction time.

TABLE III. COMPARISON OF RESPONSE TIME (IN %)

No.of rounds	DCGAN	WGAN	BERT	SPADE	Proposed
200	87.90	84.24	68.77	85.44	90.30
400	88.87	85.24	70.37	87.28	91.08
600	89.51	85.79	75.16	88.16	91.70
800	90.55	87.64	76.17	88.83	92.97
1000	91.87	88.02	77.46	89.87	94.28

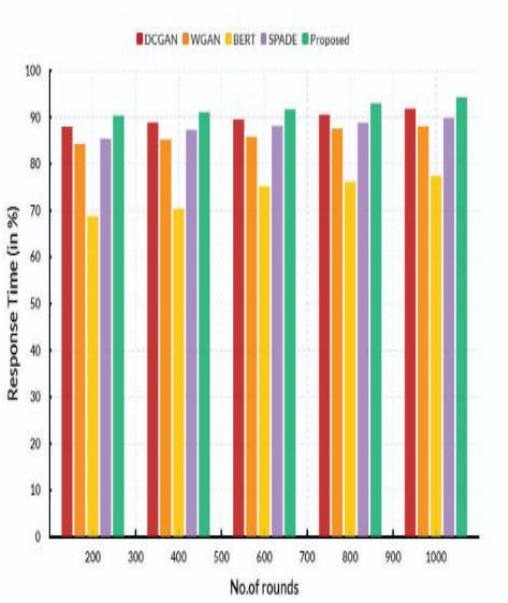

Fig. 7. Comparison of response time

Security experts can also train reacting to possible security threats by simulating real-world situations using simulations made possible by generative AI. This can enhance the efficacy of security measures and assist in identifying possible weaknesses. Lastly, generative AI can be used to identify and stop malicious software and other hazards, assisting in halting damage brought on by recently created dangers. All things considered, generative AI has the potential to be an effective instrument for improving threat intelligence and cyber security protocols. Organizations can detect malicious threats more rapidly and respond to them as efficiently as feasible with the use of generative AI. By using this data, firms may keep ahead of possible threats and modify their current cyber defense strategies. Additionally, generative AI can identify weaknesses in current networks and systems, assisting in their most effective patching and protection. Generative AI in threat intelligence and cyber security systems can help businesses stay safe, stop cyber attacks, identify them fast, and react to them successfully.

V. CONCLUSION

It has been shown that generative AI is a useful tool for improving cyber security and threat intelligence. In addition to generating creating

datasets for machine learning algorithms to train, generative AI may also be used to enhance data and improve the detection of malicious or unusual activities.

It can also be used to find patterns in data that hasn't been classified yet, which improves threat detection accuracy. Furthermore, current cyber security systems can be made more effective with the usage of generative AI. Generative AI is becoming a key instrument for the future of cyber security because of its capacity to enhance threat intelligence and cyber security protocols. This kind of AI is capable of simulating malevolent actors, detecting changing trends and patterns, and producing both positive and negative threat information. Additionally, it can be used to generate false positives and negatives on a massive scale, improving network readiness and protection against current and potential threats. To guarantee a better response and more potent countermeasures, AI-based systems can also dynamically modify the threat intelligence and response measures' response times. Additionally, generative AI can aid in defense against malevolent actions and efforts. It can assist in flagging potentially harmful behaviours or those connected to dubious entities by recognizing patterns and correlations amongst datasets.

REFERENCES

[1]. Dhoni, P., & Kumar, R. (2023). Synergizing Generative AI and Cybersecurity : Roles of Generative AI Entities, Companies, Agencies, andGovernment in Enhancing Cyber security .

[2]. Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). FromChatGPT to ThreatGPT: Impact of generative AI in cyber security andprivacy. IEEE Access.

[3]. Teichmann, F. (2023). Ransomware attacks in the context of generative artificial intelligence—an experimental study. International Cybersecurity Law Review, 1-16.

[4]. Striuk, O. S., & Kondratenko, Y. P. (2023). Generative Adversarial Networks in Cyber security : Analysis and Response. In ArtificialIntelligence in Control and Decision-making Systems: Dedicated toProfessor Janusz Kacprzyk (pp. 373-388). Cham: Springer NatureSwitzerland.

[5]. Chaudhary, G., Srivastava, S., & Khari, M. (2023). Generative Edge Intelligence for Securing IoT assisted Smart Grid against Cyber-Threats. International Journal of Wireless & Ad HocCommunication, 6(1).

[6]. Wach, K., Duong, C. D., Ejdys, J., Kazlauskaitė, R., Korzynski, P.,Mazurek, G., ... & Ziemba, E. (2023). The dark side of generativeartificial intelligence: A critical analysis of controversies and risks ofChatGPT. Entrepreneurial Business and Economics Review, 11(2), 7-24

[7]. Dhanasekaran, S., & Ramesh, J. (2021). Channel estimation using spatial partitioning with coalitional game theory (SPCGT) in wirelesscommunication. Wireless Networks, 27, 1887-1899.

[8]. Gupta, K., Jiwani, N., & Afreen, N. (2023). A Combined Approach ofSentimental Analysis Using Machine Learning Techniques. Revued'Intelligence Artificielle, 37(1).

[9]. J.Logeshwaran, & T.Kiruthiga. (2022). The Smart Performance Analysis of Network Scheduling Framework for Mobile Systems inCloud Communication Networks. International Journal of Research inScience & Engineering (IJRISE), 2(01), 11–24

[10]. Ezhilarasi, K. K., & Rex, M. J. (2014). Reliable and energy-savingforwarding technique for wireless sensor networks using multipathrouting. SSRG International Journal of Computer Science andEngineering, 1(9), 11-15.

[11]. Gupta, K., Jiwani, N., Sharif, M. H. U., Datta, R., & Afreen, N. (2022, November). A Neural Network Approach For Malware Classification.In 2022 International Conference on Computing, Communication, andIntelligent Systems (ICCCIS) (pp. 681-684). IEEE.

[12]. J.Logeshwaran, & T.Kiruthiga. (2022). The Enhanced Machine Learning Model for Device Prediction in Device-To-Device (D2D)Communications. International Journal of Research in Science &Engineering (IJRISE), 2(06), 43–57

[13]. Sharif, M. H., Gupta, K., Mohammed, M. A., & Jiwani, N. (2022). Anomaly detection in time series using deep learning. InternationalJournal of Engineering Applied Sciences and Technology, 7(6), 296-305.

[14]. Cherqi, O., Moukafih, Y., Ghogho, M., & Benbrahim, H. (2023). Enhancing Cyber Threat Identification in Open-Source IntelligenceFeeds through an Improved Semi-Supervised Generative AdversarialLearning Approach with Contrastive Learning. IEEE Access.

[15]. Goel, D., Singh, D., Gupta, A., Yadav, S. P., & Sharma, M. (2023, June). An Efficient Approach For To Predict The Quality Of AppleThrough Its Appearance. In 2023 International Conference on

[16]. Computer, Electronics & Electrical Engineering & their Applications (IC2E3) (pp. 1-6). IEEE.

[17]. Purohit, K., Vats, S., Saklani, R., Kukreja, V., Sharma, V., & Yadav, S. P. (2023, July). Improvement in K-Means Clustering for InformationRetrieval. In 2023 4th International Conference on Electronics andSustainable Communication Systems (ICESC) (pp. 1239-1245). IEEE.

[18]. Chauhan, S. S., Yadav, S. P., Awashthi, S., & Naruka, M. S. (2023). Sentimental Analysis Using Cloud Dictionary and Machine LearningApproach. In Cloud-based Intelligent Informative Engineering forSociety 5.0 (pp. 157-169). Chapman and Hall/CRC.