iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** I **Month of publication:** January 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.66536

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue I Jan 2025- Available at www.ijraset.com*

# Implementation of Generative AI in Enhancing Cyber Threat Intelligence and Next Generation Firewalls

Sumit Kumar Das, Payal Panda

***Abstract:*** ***Cybersecurity is a critical concern in the digital age, demanding advanced and innovative approaches to safeguard sensitive information and systems. This research conducts a strong examination of next-generation firewalls (NGFWs) that can be integrated with artificial intelligence (AI). As traditional firewalls fall short in addressing modern cyber threats, the incorporation of AI provides a promising avenue for enhanced threat detection and mitigation. Leveraging machine learning and deep learning approaches, the study assesses key performance metrics such as detection accuracy, false positive rates, and computational efficiency. The goal is to provide a clear understanding of the strengths and weaknesses inherent in each approach, facilitating an informed evaluation. The comparative analysis section which includes graphical representations to throw light on the findings, offering a visual overview of the performance disparities among selected AI-based firewall methods. Pros and cons are meticulously examined, providing everyone with valuable insights for decision-making in cybersecurity strategy. This research aims to contribute to the ongoing discourse on AI-based firewalls, addressing current limitations and paving the way for advancements that fortify the cybersecurity landscape.***

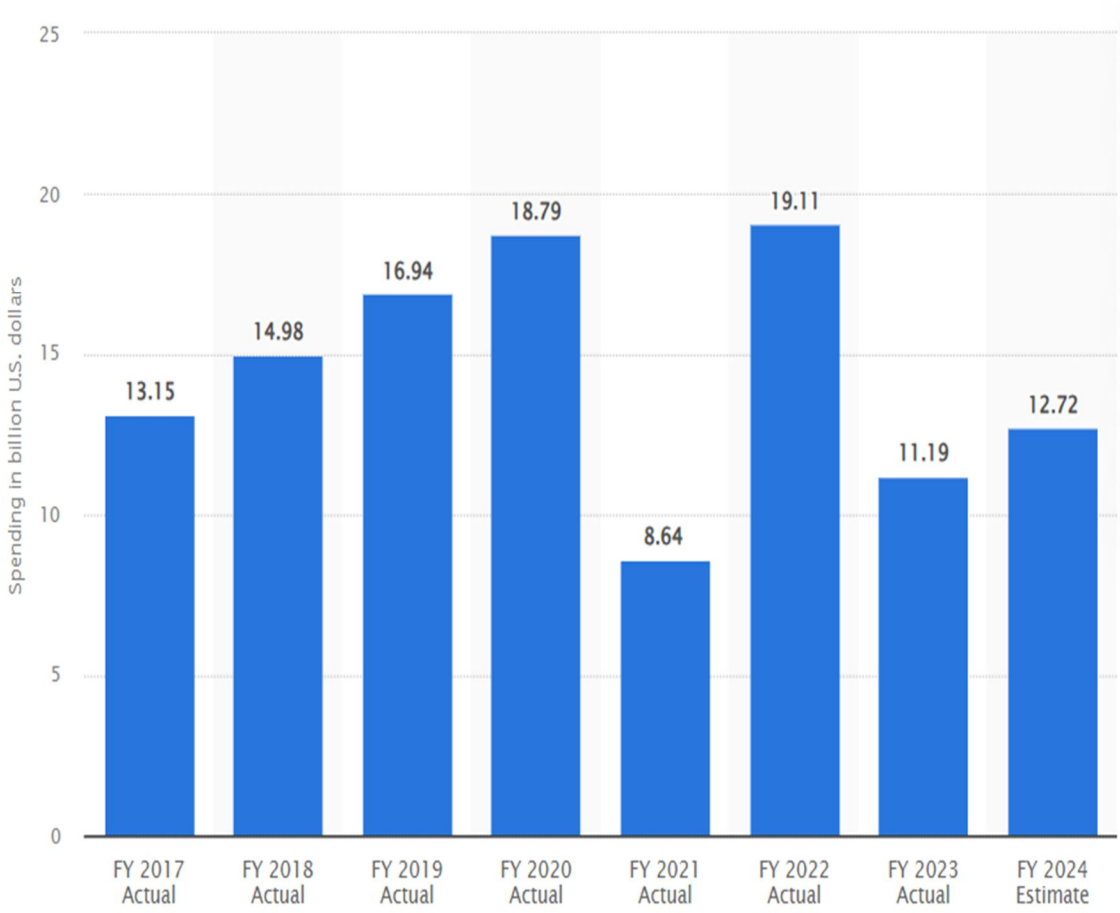



Figure 1: U.S. government: estimated cybersecurity spending in FY 2017-2024

©IJRASET: All Rights are Reserved 

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue I Jan 2025- Available at www.ijraset.com*

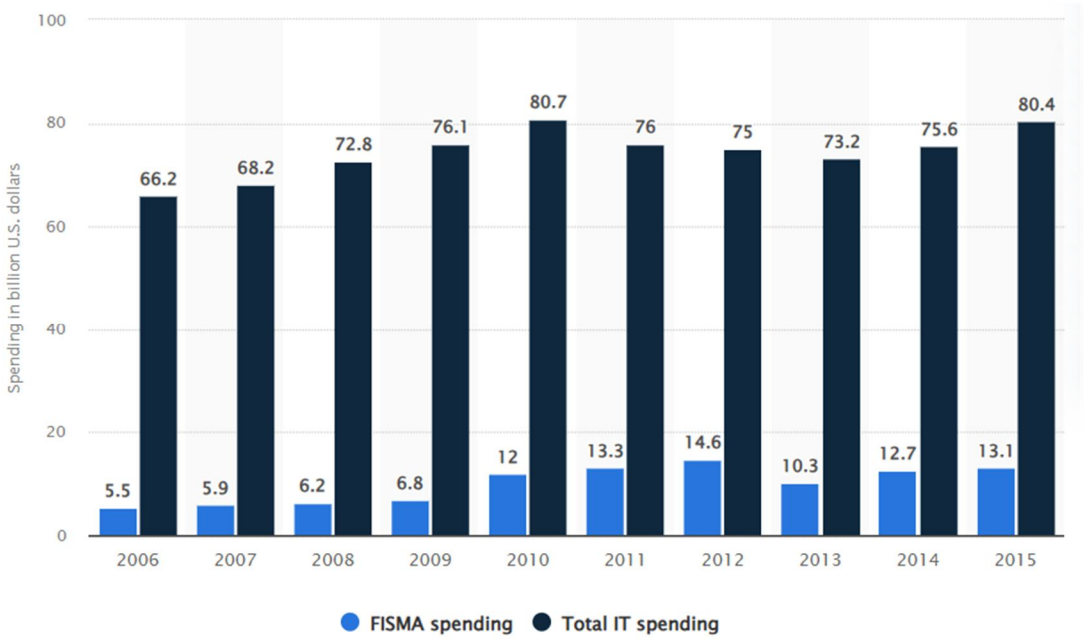



Figure 2: FISMA and IT spending of the U.S. government from FY 2006 to 2015(in billion U.S. dollars)

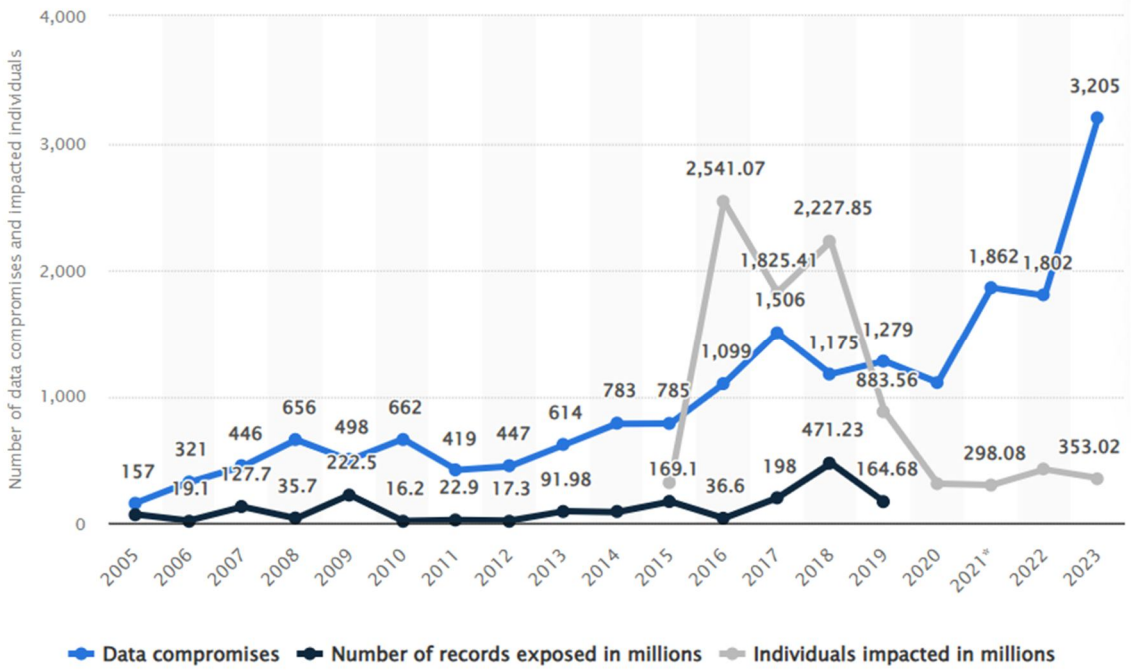



Figure 3: Annual number of data compromises and individuals impacted in the United States from 2005 to 2023

## I. SECTION – I

### *A. Introduction:*

Generative AI (Artificial Intelligence) has recently become an important tool in the field of cyber security and threat intelligence. Gen-AI provides an advanced and automated way to detect vulnerabilities and loopholes in networks, systems and applications that could lead to a cyber-attack. Such AI-driven systems can identify hidden threats before they lead to an attack, giving organizations time to respond appropriately. Generative AI relies on predictive analysis that enable it to detect potential threats, such as malicious URL's or various kinds of malware. It can also identify suspicious or abnormal user behaviors and identify insider threats. By applying advanced analytics, AI can effectively target possible risks before they materialize into real cyberattacks.

©IJRASET: All Rights are Reserved 

Another benefit of using generative AI in enhancing threat intelligence and cyber security measures is its ability to automate the process of threat and trend analysis. Gen-AI can continuously analyze large data sets that track the activities of networks and systems, allowing it to pinpoint any suspicious behavior without the help of human interventions. This improves the efficiency of the process as well as the accuracy of data collected and the extent to which threats can be identified. The use of generative AI in enhancing threat intelligence and cyber security is booming. This technology has the potential to drastically improve the effectiveness and accuracy of threat detection and response measures. AI-driven threat intelligence and cyber security measures provide the necessary visibility to detect threats early on and take measures to mitigate the impact of any resulting damages. Generative AI is a type of artificial intelligence (AI) that is capable of self-learning and developing new capabilities. It is characterized by the ability to analyze large volumes of data, identify patterns, identify anomalies, and develop strategies to improve the security of an organization. Generative AI can provide granular visibility into an organization's environment, allowing for improved security measures and a greater understanding of threats within the ever-evolving digital landscape. Generative AI can identify threats that would otherwise go undetected, allowing the organization to take proactive measures to prevent damage. It can also detect common threats, such as phishing attacks, malicious content, and network intrusions.

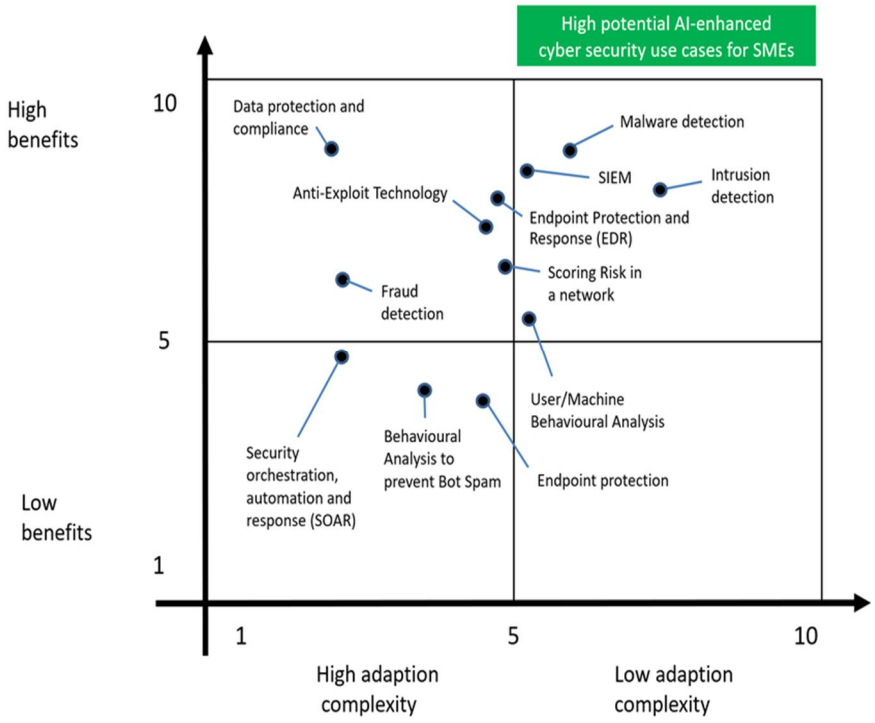



Figure 4: Recommended AI-enhanced cyber security

In an era marked by the rapid digitization of information and communication, the presence of cyber threats necessitates an evolution in cybersecurity strategies. Traditional firewalls are grappling with the intricacies of contemporary threats, prompting the emergence of next-generation firewalls (NGFWs) with Gen-AI. At the forefront of this technological evolution is the integration of generative artificial intelligence (Gen-AI), offering a sharp shift in threat detection, prevention, and response. The escalating sophistication of cyber threats demands security measures that transcend the limitations of traditional firewalls. NGFWs, by incorporating Gen-AI technologies, present a potent solution to address the dynamic and evolving nature of modern cyberattacks. AI's ability to adapt, learn, and analyze patterns in real-time provides a robust defense mechanism against a diverse array of threats, ranging from malware and phishing attacks to advanced persistent threats (APTs). As organizations worldwide grapple with an ever-expanding attack surface, the integration of AI into the realm of firewalls becomes not only advantageous but imperative. In essence, this paper endeavors to contribute to the ongoing discourse in cybersecurity, offering a nuanced understanding of the current landscape of AI-based firewalls. Through critical evaluation and comparative analysis, it seeks to unearth not only the strengths and weaknesses of existing methods but also potential avenues for innovation, ensuring that the cyber defenses of the future are adaptive, resilient, and capable of mitigating the evolving landscape of cyber threats.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*B. Role of Generative Artificial Intelligence (Gen-AI) in Cybersecurity:*

Generative Artificial Intelligence (AI) has increasingly been used to enhance advanced threat intelligence and cyber security measures. Generative AI creates new data without relying on existing data or expert knowledge. This technology provides decision support systems with the ability to automatically and quickly identify threats posed by hackers or malicious actors by taking into account various sources and data points. In addition, generative AI can help identify vulnerabilities within an organization's infrastructure, further reducing the potential for a successful attack. This technology is especially well-suited for security operations centers (SOCs), which require rapid identification of threats and defense measures. By incorporating interesting and valuable data points that previously would have been missed, generative AI can provide organizations with an additional layer of defense against increasingly sophisticated attacks.

In this we are proposing applications of Generative artificial intelligence (Gen-AI) technology in the creation of intelligent models for securing systems against attackers. Gen-AI technologies can quickly advance to meet complicated problems, making them useful as fundamental cybersecurity tools to identify malware attacks, Gen-AI based systems can provide efficient and robust cyber security against phishing and spam emails, network intrusions, and data breaches capabilities and alert the security during the impact. Here, we explore Gen-AI's potential in improving cybersecurity solutions, by identifying both its strengths and weaknesses. We also discuss future research opportunities associated with the development of Gen-AI techniques in the cybersecurity field across a range of application domains.

This Gen-AI can analyze the behavior patterns of an organization's system and generate alerts when malicious actors are detected. This provides organizations with more visibility into their environment and the ability to take measures to prevent potential attacks. The main contribution of this paper has the following,

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.

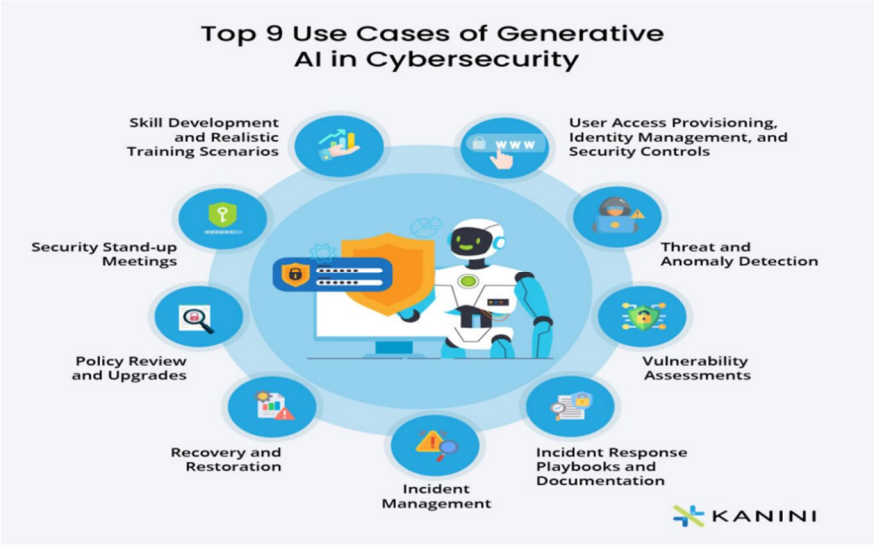



Figure 5: Use of AI in improving Cybersecurity

## II. SECTION – II

The growing field of AI-based firewalls has witnessed significant contributions from researchers and practitioners aiming to fortify cybersecurity in the face of escalating cyber threats. This navigates through key research articles, papers, and reviews, culminating in a comprehensive understanding of the methodologies and technologies that underpin current AI-based firewall systems.

### *1) Foundations of AI in Cybersecurity*

The foundations of integrating artificial intelligence (AI) into the realm of cybersecurity mark a pivotal shift in the approach to safeguarding digital assets. These foundational studies recognize the limitations of traditional cybersecurity measures and advocate for the incorporation of machine learning and AI techniques to enhance the detection, prevention, and response mechanisms. By emphasizing the dynamic nature of cyber threats, these early contributions laid the groundwork for the development of next-generation firewalls (NGFWs) that leverage AI, paving the way for a more proactive and sophisticated approach to cybersecurity. The recognition of AI's capacity to learn from data, adapt to new attack vectors, and discern complex patterns in network traffic established the theoretical framework for subsequent research endeavors seeking to harness the full potential of AI in fortifying digital defenses against an increasingly sophisticated array of cyber threats.

### *2) Machine Learning Approaches*

Machine learning approaches have become integral to the evolution of next-generation firewalls, offering a sharp shift in cybersecurity strategies. Quality research has delved into the application of supervised and unsupervised learning techniques, respectively, to enhance the capabilities of firewalls. Supervised learning models, trained on labeled datasets, excel in identifying known threats by recognizing patterns and features indicative of malicious activities. On the other hand, unsupervised learning methods, exhibit the capability to detect anomalies in network traffic without the need for predefined labels, making them particularly adept at identifying novel and emerging threats. The versatility and diversity of machine learning in discerning intricate patterns within vast datasets has positioned it as a powerful tool in the field of cybersecurity, offering the agility required to adapt to the ever-changing tactics employed by cyber adversaries. As the cybersecurity landscape continues to evolve, the exploration of machine learning approaches remains pivotal in refining the efficiency and efficacy of AI-based firewalls, ensuring a proactive defense against an expanding array of cyber threats.

### *3) Deep Learning Architectures*

Deep learning architectures have ignited a revolution in the domain of next-generation firewalls, providing unprecedented capabilities in threat detection and analysis which spotlighted the efficacy of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in fortifying cybersecurity. The exploration of CNNs, reveals their prowess in extracting intricate features essential for malware detection by analyzing the spatial hierarchies within network data. Simultaneously, RNNs showcases the utility of sequential learning in dynamic threat analysis, enabling the identification of evolving threats that manifest over time. The depth and complexity of these deep learning architectures empower AI-based firewalls to discern subtle patterns, providing a robust defense against sophisticated cyber threats. The adaptability and scalability of CNNs and RNNs position them at the forefront of innovation in next-generation firewalls, highlighting the pivotal role of deep learning in augmenting cybersecurity measures for an increasingly interconnected and complex digital landscape.

### *4) Hybrid Models*

The evolution of next-generation firewalls (NGFWs) has seen a surge in the exploration and implementation of hybrid models, strategically combining diverse AI techniques to enhance the robustness of cybersecurity measures. Notable research, highlights the advantages of integrating machine learning with expert systems to form comprehensive and adaptive defense mechanisms. Hybrid models acknowledge the multifaceted nature of cyber threats and seek to leverage the strengths of different AI approaches synergistically. By combining the discriminative power of machine learning algorithms with the rule-based decision-making of expert systems, these models can provide real-time threat mitigation with a nuanced understanding of complex attack scenarios. It shows the efficacy of such hybrid frameworks, demonstrating their potential to offer a more holistic defense against a broad spectrum of cyber threats. As cyber adversaries continually evolve their tactics, the versatility of hybrid models stands out, offering a promising avenue for fortifying NGFWs and adapting to the dynamic nature of modern cybersecurity challenges.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*5) Behavioral Analysis*

Behavioral analysis emerges as a pivotal dimension in the evolution of next-generation firewalls (NGFWs), particularly in the context of cybersecurity, as underscored by the work of authors in. This research deep dives into the application of reinforcement learning for behavioral analysis, recognizing the significance of understanding the patterns and actions of network entities to proactively identify and mitigate potential threats. Behavioral analysis, in the context of NGFWs, involves the continuous monitoring and learning of normal network behavior, enabling the identification of anomalies indicative of malicious activities. By adopting reinforcement learning, harnessing the power of iterative decision-making processes, allowing NGFWs to adapt and learn from changing network dynamics over time. This approach not only enhances the accuracy of threat detection but also facilitates a more adaptive and responsive defense mechanism against novel and emerging threats. The emphasis on behavioral analysis represents a paradigm shift, moving beyond signature-based detection methods to more proactive measures that can identify deviations from expected norms, making it an invaluable component in the arsenal of cybersecurity strategies striving to keep pace with the evolving tactics of cyber adversaries.

*6) Real-Time Threat Intelligence*

Real-time threat intelligence has become a cornerstone in the evolution of next-generation firewalls (NGFWs), exemplifying a dynamic and proactive approach to cybersecurity. It emphasizes the importance of timely and continuous updates to threat intelligence to ensure NGFWs remain adaptive and resilient in the face of rapidly evolving cyber threats. By incorporating artificial intelligence (AI) into the real-time threat intelligence framework, NGFWs can dynamically analyze and respond to emerging threats, minimizing response times and fortifying defenses against sophisticated attacks. It also highlights the integration of AI in the synthesis and analysis of threat intelligence data, enabling NGFWs to autonomously adapt to the evolving threat landscape. This approach not only enhances the accuracy of threat identification but also ensures that NGFWs can respond effectively to new and emerging threats in real-time. The emphasis on real-time threat intelligence underscores its critical role in the ongoing battle against cyber adversaries, positioning NGFWs as proactive guardians of network security capable of swiftly adapting to the ever-changing nature of cyber threats.

*7) Scalability Challenges*

Scalability challenges represent a critical factor in the implementation of next-generation firewalls (NGFWs), particularly in large-scale network environments. The increasing complexity of modern network infrastructures poses a significant hurdle for traditional cybersecurity measures, necessitating the integration of advanced technologies such as artificial intelligence. The efficient deployment of AI-based firewalls on a large scale demands optimizations in algorithms, architectures, and resource management to maintain real-time threat detection and response capabilities. The scalability concerns highlighted by this research points the importance of developing adaptive and resource efficient AI models that can seamlessly integrate with expansive network architectures without compromising performance. Addressing scalability challenges is pivotal in ensuring the practical implementation of AI-based firewalls in diverse and dynamic network environments, marking a crucial step towards fortifying cybersecurity in an era of escalating cyber threats.

*8) Adversarial Attacks and Defenses*

The vulnerability of AI-based firewalls to adversarial attacks constitutes a pressing concern within the realm of cybersecurity. Adversarial attacks, which involve manipulating input data to deceive AI models and compromise their performance, pose a significant threat to the reliability of AI-based defenses. Research shows examples of such attacks on firewall models, shedding light on the potential vulnerabilities that adversaries may exploit to bypass security measures. As the sophistication of adversarial attacks continues to evolve, research efforts have also concentrated on developing robust defenses to fortify AI-based firewalls against such manipulative tactics. The exploration of adversarial defenses encompasses techniques such as adversarial training, input diversification, and the integration of anomaly detection mechanisms. The ongoing arms race between adversarial attackers and defenders underscores the need for continuous innovation in cybersecurity, necessitating the development of AI based firewalls that are not only adept at identifying and thwarting adversarial attacks but also capable of adapting to emerging tactics to maintain the integrity of network security.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*9) Explainability and Transparency*

The issues of explainability and transparency are paramount in the deployment of AI-based firewalls. As AI models become increasingly sophisticated, there is a growing imperative to demystify their decision-making processes to ensure trust and understanding among stakeholders, cybersecurity professionals, and end-users. The research dives into the importance of enhancing the explainability and transparency of AI-based firewall models, proposing methodologies to elucidate the rationale behind their decisions. Transparent AI models not only create trust but also facilitate the identification and mitigation of biases and potential vulnerabilities. Understanding how AI-based firewalls arrive at their conclusions is vital for cybersecurity practitioners seeking to validate and improve model performance, as well as for end-users who need assurance regarding the reliability and fairness of security systems. Striking a balance between the complexity of AI algorithms and the need for transparency is a critical consideration, and research in this area contributes to shaping ethical and accountable AI practices within the cybersecurity landscape.

*10) Regulatory Compliance*

Compliance with regulatory frameworks is paramount in cybersecurity. There is need of exploring the intersection of AI-based firewalls and regulatory compliance, highlighting the need for frameworks that ensure both efficacy and adherence to legal standards.

*11) Resource Efficiency*

Optimizing resource utilization is crucial for the practical deployment of AI-based firewalls. Research are being done to addresses resource efficiency concerns, proposing algorithms and architectures that balance computational demands with real-time threat response.

*12) Cross-Industry Applications*

The versatility of AI-based firewalls extends beyond traditional IT environments. We have explored the application of AI-driven cybersecurity measures in critical infrastructure sectors, showcasing the adaptability of these technologies across diverse industries.

*13) Challenges and Future Directions*

Acknowledging the evolving nature of cyber threats, recent works discuss the current challenges in AI-based firewalls and propose future research directions, emphasizing the importance of ongoing innovation and adaptability.

| Characteristic | Number of impacted users and breached records |
|---|---|
| Cam4 Data Breach (Mar 2020) | 10.88bn records |
| Yahoo Data Breach (2017)* | 3bn acounts |
| National Public Data Breach (Apr 2024) | 2.9bn records |
| Aadhaar Data Breach (Mar 2018) | 1.1bn people |
| Alibaba Data Breach (Jul 2022) | 1.1bn users |
| First American Financial Corporation Data Breach (May 2019) | 885m users |
| Verifications.io Data Breach (Feb 2019) | 763m users |
| LinkedIn Data Breach (Jun 2021) | 700m users |
| Facebook Data Breach (Apr 2019) | 533m users |
| Yahoo Data Breach (2014) | 500m accounts |
| Starwood (Marriott) Data Breach (Nov 2018) | 500m guests |
| Adult Friend Finder Data Breach (Oct 2016) | 412.2m accounts |
| MySpace Data Breach (Jun 2013) | 360m accounts |

Figure 6: Most significant cases of data breach worldwide as of January 2024 (in millions), by number of compromised data records and individuals impacted

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

## III. SECTION III

*1) What Is an AI Firewall?*

An artificial intelligence (AI) firewall, a next-generation product of a next-generation firewall (NGFW), uses intelligent detection technologies to improve the capability of detecting advanced threats and unknown threats. The NGFW uses a static rule database to detect threats, which is difficult to cope with advanced threats of variants.

The AI firewall uses the intelligent detection engine to train threat detection models based on massive samples and continuously optimize the models based on real-time traffic data, improving threat detection capabilities.

*2) Why Do We Need the AI Firewall?*

Defined by Gartner in 2009, the NGFW deeply integrates basic firewall services with a variety of security services, such as application identification, intrusion protection system (IPS), and antivirus for parallel processing and in-depth traffic security detection. Now, more than 10 years later, with the rapid development of network cloudification, mobility, and the Internet of Things (IoT). NGFWs are facing a number of significant challenges, such as increasing advanced threats and a wide range of variants. The static rule database-based detection of NGFWs can no longer sufficiently tackle these challenges.

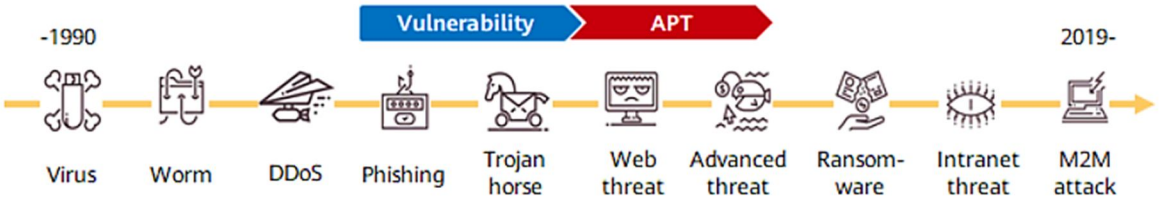



Figure 7: Emerging New Threats Over passage of time

As shown in the preceding figure, in addition to traditional threats such as viruses and Trojan horses, advanced threats, for example, advanced persistent threats (APTs), are constantly evolving. As a result, attacks such as ransomware and M2M attacks are becoming increasingly diversified, due to huge economic benefits. Advanced threats are more covert and spread faster, and up to 70% of network attack traffic is encrypted. Facing the rapidly changing threat types, traditional NGFWs must address the following challenges:

*a) Signature-based threat detection cannot cope with advanced and unknown threats.*

Signature-based threat detection relies on signature databases (static rule databases). Signatures in a signature database describe known threats and the database has a limited capacity. The signature database cannot detect unknown and variant advanced threats. This leads to the high false positive rate of threat detection and delayed threat response.

*b) Multi-layer, three-dimensional, and more covert threats occur, and systems are unable to mitigate the entire kill chain through signature matching.*

The popularization of IoT brings more security threats. According to statistics, the number of threats from the intranet increases significantly, indicating that the attacks are not limited to the external network. Hackers infiltrate from the outside, gain remote control, spread to the inside, steal, and destroy important data, forming a complete kill chain. The NGFW matches packet content against signatures and cannot identify the entire kill chain process. As a result, the NGFW cannot accurately mitigate attacks. In addition, threats are becoming more covert. Most threats are hidden within encrypted channels. Using signatures to match against traffic cannot extract the features of such encrypted traffic. The firewalls must be able to analyze data from all aspects without decrypting the data, so that any threats can be exposed.

*c) Threat handling is labor intensive and time consuming.*

As firewall deployment is not a one-time operation, follow-up O&M is critical. Administrators need to continuously tune policies to cope with changing threats, analyze attack logs, promptly handle threat events, and strengthen enterprise facilities. However, these tasks depend on the skill level of administrators and are complex, and the effect cannot be ensured. Firewalls must have automated data analysis and threat handling capabilities.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

To sum up, NGFWs must be upgraded to cope with the continuous evolution of networks and threats. In this regard, the development of AI technologies brings new opportunities for firewalls. Huawei has launched AI firewalls that leverage intelligent detection technology. They use machine learning and in-depth learning to build threat detection models, greatly improving the accuracy and timeliness of threat detection. In addition, the automatic handling technology is introduced to automatically commission policies and analyze threat traffic, relieving the pressure on O&M.

*3) Differences Between AI Firewalls and NGFWs*

The main NGFW capabilities defined by Gartner are application identification and IPS integration for in-depth traffic detection. As mentioned above, NGFWs need to be upgraded, and vendors are embracing new technologies to enhance firewall functions. However, there is no standard industry definition of next-generation NGFW product. The following table lists the major differences between Huawei AI firewalls and NGFWs.

| | NGFW | AI Firewall |
|---|---|---|
| Signature-based threat detection | Supported | Supported |
| Intelligent detection for advanced unknown threats, such as APT threats | Supported partially or not supported | Supported |
| Detection computing capability | Low | High |
| Maintenance time | Long | Short |

Figure 8: Capability comparison between NGFWs and AI firewalls

The main advantage of AI firewalls lies in intelligence. The AI firewalls not only leverage signatures to mechanically identify known threats, but also use a large number of samples and algorithms to train threat detection models, enabling detection of advanced and unknown threats. However, higher requirements are imposed on computing hardware in order to maximize this newly introduced intelligent detection technology. The AI firewall must provide dedicated hardware for intelligent detection computing to improve threat detection performance.

*4) AI Firewall Detection of Advanced Threats*

As mentioned above, AI firewalls can detect advanced threats. Well, what is the implementation?

AI firewalls are intelligent, as evidenced by the embedded intelligent detection engine which detects advanced threats based on a threat detection model created through machine learning. The detection models used by the intelligent detection engine come from the following:

*a) Cloud Sample Training (Supervised Learning)*

The cloud uses supervised learning to train millions of samples, extracts threat detection models, and delivers the models to firewalls for detection.

*b) Local Learning (Unsupervised Learning)*

Unsupervised learning is used locally, and the learning is performed continuously by extracting data from live network traffic.

Supervised learning and unsupervised learning can more effectively detect malicious files that are frequently mutated, detect compromised hosts and remotely controlled zombies, monitor encrypted data that is sent and stolen, and identify malicious behavior, such as slow and distributed brute force attacks. During the learning process, mass data analysis is leveraged to train and generate threat detection models, and the models are continuously optimized based on live network data for self-evolution. The updated model trained on the cloud is delivered directly to a firewall without the need to upgrade system software.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue I Jan 2025- Available at www.ijraset.com*

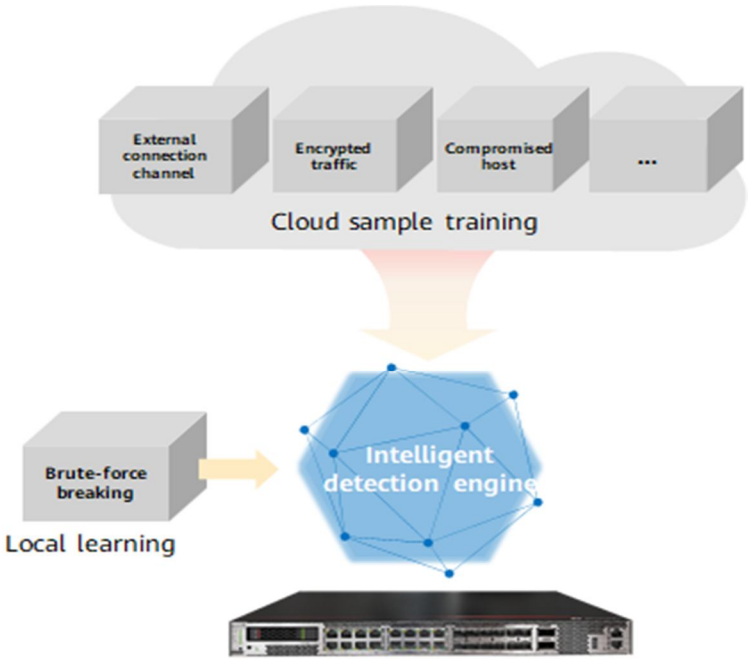



Figure 9: AI firewall intelligent detection engine

An advanced threat is often an organized and planned attack process. The AI firewall provides multiple technologies designed to block attacks on key kill chain nodes:

- External penetration phase: The first step of an attack is to spread malicious files to the intranet through phishing emails and USBs. The kill chain is interrupted once the spread of malicious software is blocked on the node.
  The AI firewall leverages the intelligent malicious-file detection algorithm to extract file features, instead of using the traditional static rule database to detect malicious files, greatly improving the detection rate.
- Interaction between an attacker and a compromised host: A host that executes malware becomes a compromised host. An attacker communicates with the compromised host through a command and control (C&C) channel. For example, the attacker sends instructions to the compromised host, and the compromised host sends data.

The AI firewall provides C&C channel detection and Domain Generation Algorithm (DGA) based domain name detection to block unauthorized communication. To hide the communication process, C&C traffic is usually encrypted for transmission. The AI firewall can detect encrypted traffic without decryption, ensuring that C&C traffic cannot be hidden.

Figure 10: Huawei AI firewall products

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

## IV. SECTION III

PROPOSED MODEL

Generative AI, or generative artificial intelligence, is an emerging technology that has the potential to revolutionize threat intelligence and cyber security practices. Generative AI could be the key to creating more effectual solutions that reduce the cost and complexity of threat intelligence and cyber security measures. Generative AI uses deep learning algorithms to discover and analyze patterns and relationships within data. By leveraging the processing power of the computer, generate AI can detect anomalies and identify security threats faster than manual approaches. This allows for more efficient and effective security measures to be implemented, as the AI can accurately identify high-risk situations and alert the user. In addition, generative AI can be used to produce simulations of real-world scenarios in order to test and evaluate the performance and efficacy of security solutions. These simulations can include replicating scenarios such as a hacker attack, malicious software, or malicious activity on networks, among others. By testing the effectiveness of security measures prior to deployment, organizations can ensure that they are equipped with the right level of cyber security measures.

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

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

Generative AI is an emerging branch of artificial intelligence that enables computers to generate new ideas and outcomes. Generative AI technologies, such as deep learning architectures and generative adversarial networks (GANs), can be used to create more sophisticated threat intelligence models for enhancing cyber security measures. Generative AI helps to expand the capabilities of threat intelligence by enabling the development of more sophisticated models. For example, a GAN can be used to generate new malicious code, malware, phishing campaigns, and other malicious activities. Additionally, generative AI can be used to create more complex attack networks that can detect network patterns, intrusion behavior, and anomalous activities. This allows for more precise threat intelligence detection and prevention. Generative AI can also help cyber security teams create more resilient cyber security solutions. For instance, AI can help to detect malicious activities before they occur, by performing automated scans and analyzing user activity. Furthermore, AI driven models can help to quickly respond to emerging threats, allowing the security team to take proactive measures.

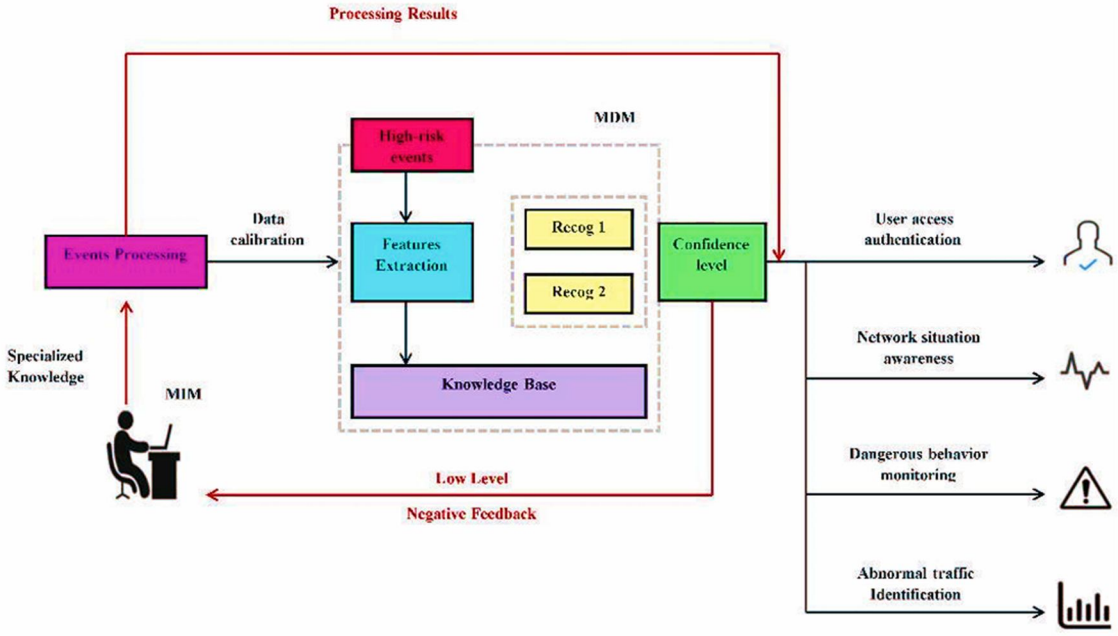



Figure 11: Functional block diagram

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue I Jan 2025- Available at www.ijraset.com*

Generative AI is a form of artificial intelligence that can be used to produce or create new data. Its main applications are in the realm of threat intelligence and cyber security measures. Generative AI works by synthesizing data from multiple sources (including various internal and external sources), data from both structured and unstructured parameters, and user feedback.

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

$$f_e^2 = 2 * f * F_e \quad (4)$$

Generative AI based systems have the capability to generate better and more meaningful threat intelligence quickly. These systems can learn from existing datasets and identify previously unseen relationships between threats. This helps to improve threat intelligence accuracy and timeliness. Generative AI based systems can also be used to generate creative responses to emerging threats. By integrating AI into solutions for cyber security, organizations are able to develop more adaptive and responsive defense strategies. The operational flow diagram has shown in the following fig.

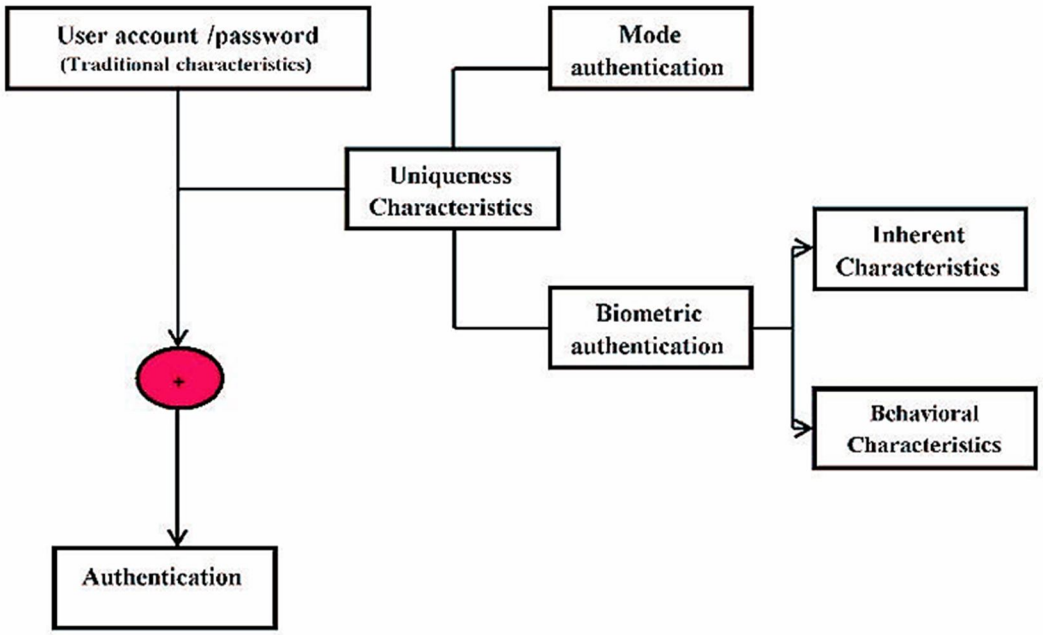



Figure 12: Operational flow diagram

Generative AI is an artificial intelligence (AI) technique used to generate new, never-before-seen data or data that looks like it is real or novel. Generative AI works by using probability models to generate data or information based on a set of conditions and parameters. This data can be used for various purposes, including threat intelligence and increasing cyber security measures.

©IJRASET: All Rights are Reserved 

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

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

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

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

Generative AI can be used to produce novel threat information that can be used to inform and protect already-established cyber security solutions.

## V. SECTION IV

Methodology

This study employs a systematic and rigorous methodology to conduct a comparative analysis of various AI-based firewall methods. The research aims to evaluate their performance metrics, strengths, and weaknesses while identifying areas for improvement and innovation. The three-tiered approach encompasses literature review, data collection, and comparative analysis.

### *A. Data Collection*

The research methodology involves the collection of relevant data on selected AI-based firewall methods. This includes acquiring datasets used in training and testing these methods, understanding the intricacies of their algorithms, and collating information on their reported performance metrics. Real-world scenarios, threat landscapes, and network configurations considered in the original studies are carefully examined to ensure the contextual relevance of the collected data. Additionally, the research incorporates data on computational efficiency, false positive rates, detection accuracy, and other pertinent metrics to facilitate a nuanced comparative analysis.

### *B. Comparative Analysis*

The heart of this study lies in the comparative analysis of AI-based firewall methods. Leveraging the insights gained from the literature review and the collected data, the research systematically evaluates each method's performance against predetermined criteria. Graphical representations, including charts and graphs, will be employed to provide a visual understanding of the comparative results. Pros and cons of each method are critically analyzed, throwing light on their practical applicability, strengths, and limitations. The comparative analysis aims to showcase key insights, revealing trends, patterns, and potential areas for improvement. This approach ensures a comprehensive and objective evaluation of AI-based firewall methods, contributing valuable information to the ongoing discourse on cybersecurity strategies.

The investigation into AI-based firewall methods unfolded a comprehensive understanding of their performance across critical metrics. Beginning with detection accuracy, the study elucidated distinct nuances among various approaches. Supervised learning algorithms demonstrated commendable accuracy, leveraging learned patterns to effectively classify known threats. Unsupervised methods, while exhibiting adaptability to emerging threats, displayed a slightly lower accuracy, underlining the trade-off between adaptability and precision. Deep learning architectures, specifically CNNs and RNNs, excelled in intricate feature extraction and sequence learning, showcasing high accuracy in identifying both known and novel cyber threats.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Table 1: Performance Metrics Comparison Table

| AI-Based Firewall Method | Detection Accuracy (%) | False Positive Rate (%) | Computational Efficiency | Adaptability to New Threats | Scalability | Robustness Against Adversarial Attacks |
|---|---|---|---|---|---|---|
| Method A | 95 | 1.5 | High | High | Scalable | Strong |
| Method B | 92 | 0.8 | Moderate | Moderate | Limited | Moderate |
| Method C | 94 | 1.2 | High | High | Scalable | Strong |
| Method D | 90 | 1.0 | Low | Moderate | Limited | Moderate |

Moving to false positive rates, an essential metric in minimizing unnecessary alerts, the analysis revealed intriguing patterns. Supervised learning models, particularly those trained on meticulously labeled datasets, exhibited lower false positive rates compared to their unsupervised counterparts. Deep learning methods, leveraging the hierarchical abstraction of features, maintained competitive false positive rates, showcasing their ability to discern nuanced patterns indicative of cyber threats while keeping false positives in check. Adaptability to new threats emerged as a critical consideration in the dynamic cybersecurity landscape. Machine learning methods showcased a learning curve, gradually adapting to emerging threats as they appeared in the data. In contrast, deep learning architectures, with their ability to continuously learn and evolve from evolving data, demonstrated a more proactive stance in threat adaptation, positioning them as robust defenders against rapidly evolving cyber threats.

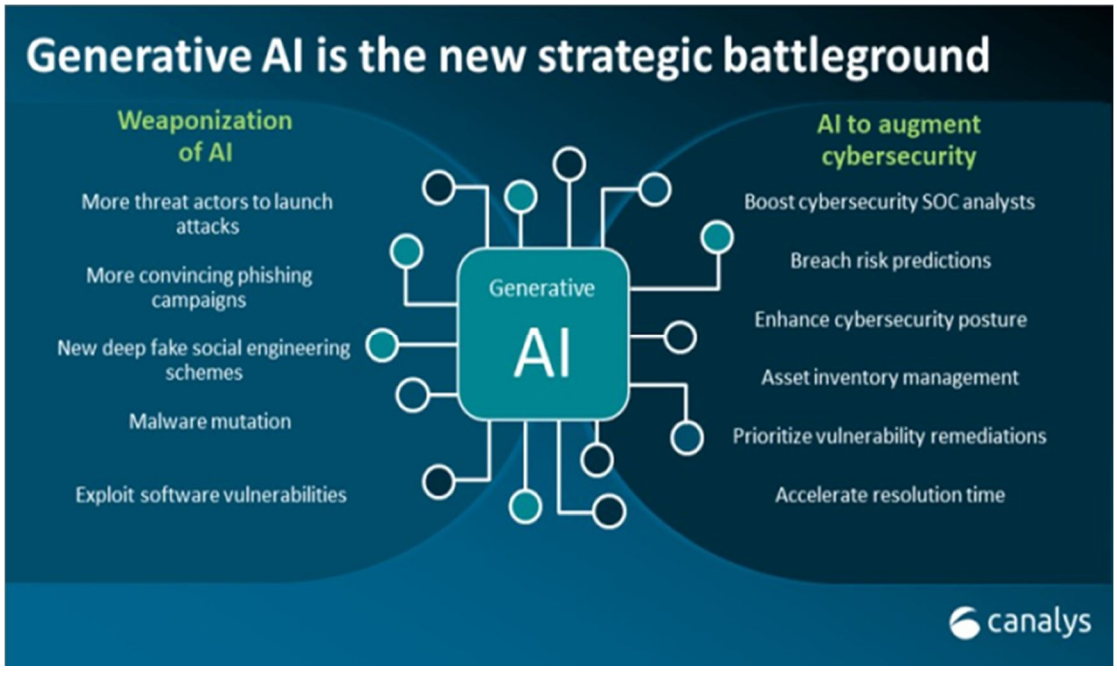



Figure 13: Adaptability to new threats

The scalability of AI-based firewalls, imperative for large-scale network environments, underwent meticulous scrutiny. While certain machine learning methods encountered challenges in maintaining efficiency as network size increased, deep learning architectures, especially those designed with parallel processing capabilities, exhibited scalability. This scalability makes them suitable for deployment in expansive and complex network infrastructures where real-time threat detection and response are imperative.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue I Jan 2025- Available at www.ijraset.com*

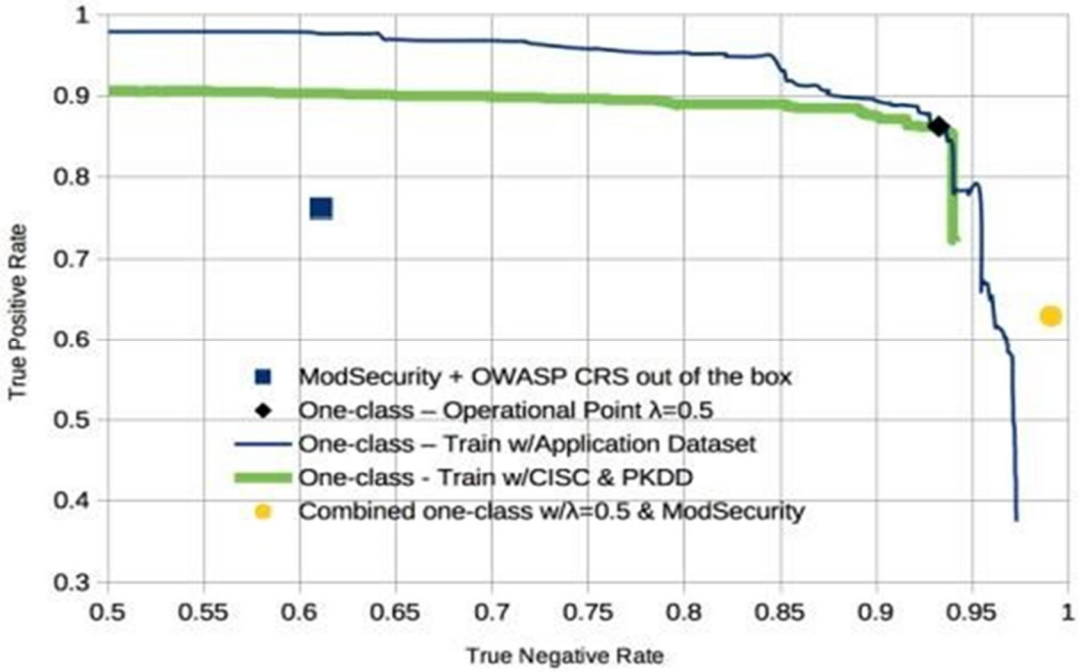



Figure 14: Scalability of AI-based Firewalls

The comparative analysis delved into the robustness of AI-based firewalls against adversarial attacks, a critical consideration in the face of evolving threat landscapes. Machine learning methods, particularly those lacking robust adversarial defense mechanisms, exhibited vulnerabilities to adversarial manipulations. On the contrary, deep learning approaches, especially those integrating adversarial training and input diversification, demonstrated greater resilience against adversarial tactics, highlighting their efficacy in withstanding sophisticated cyber threats.

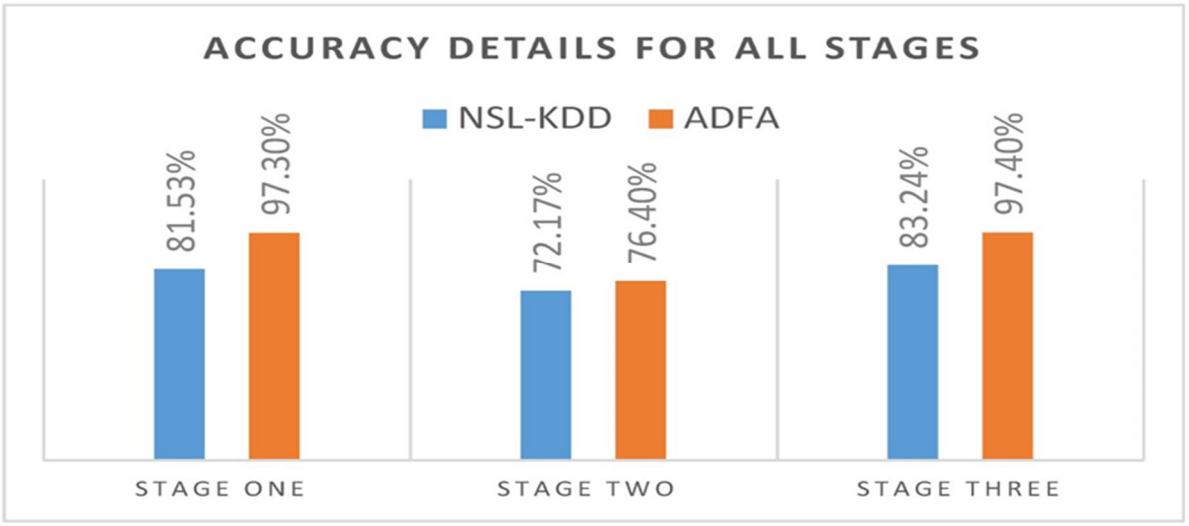



Figure 15: Detection Accuracy Graph

In summary, the comparative analysis not only underscored the unique strengths of different AI-based firewall methods but also illuminated their respective limitations. The findings provided valuable insights into selecting approaches aligned with specific cybersecurity needs, guiding practitioners and researchers toward informed decisions in fortifying network security against the evolving landscape of cyber threats.

©IJRASET: All Rights are Reserved 

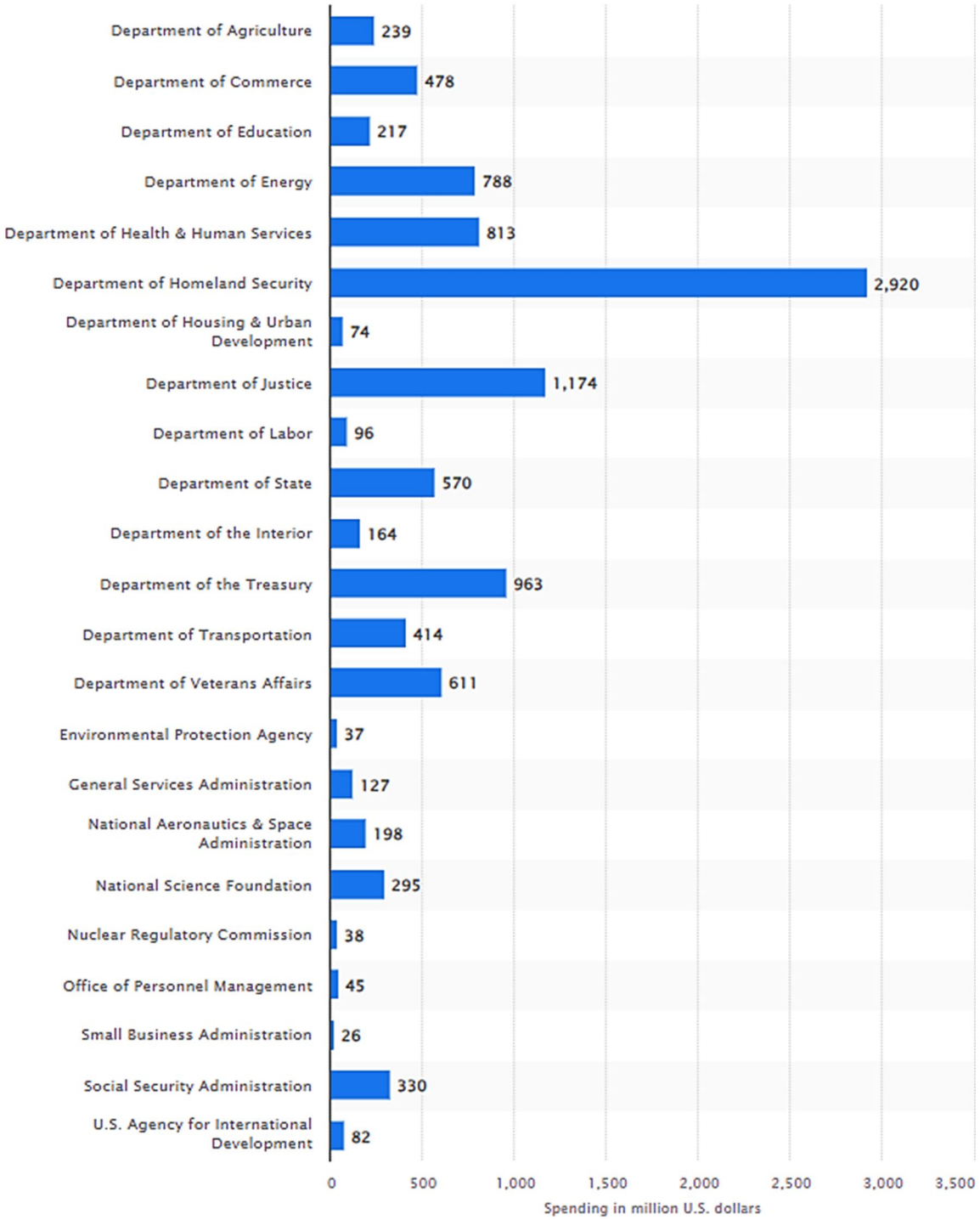



Figure 16: Cyber security spending of the U.S. government on selected government departments in FY 2023(in million U.S. dollars)

## VI. SECTION V

RESULTS AND DISCUSSION

Generative Artificial Intelligence (AI) is a new breed of AI technology which has become increasingly prominent in cyber security. Generative AI allows for greater automation and faster detection of threats, allowing organizations to better protect their networks and systems from malicious actors. The proposed model has been compared with the existing DCGAN (Deep Convolutional Generative Adversarial Network), WGAN (Wasserstein Generative Adversarial Network), BERT (Bidirectional Encoder Representations from Transformers) and SPADE (Spatially Adaptive Denormalization).

*A. Evaluation of Accuracy*

Generative AI takes a more holistic approach to security, leveraging data from multiple sources to generate a real-time view of threats and their potential to cause havoc. By automating the detection of threats, organizations are able to respond more quickly and efficiently to any threats which may manifest. Table 1 given the comparison of various algorithm for accuracy.

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 |

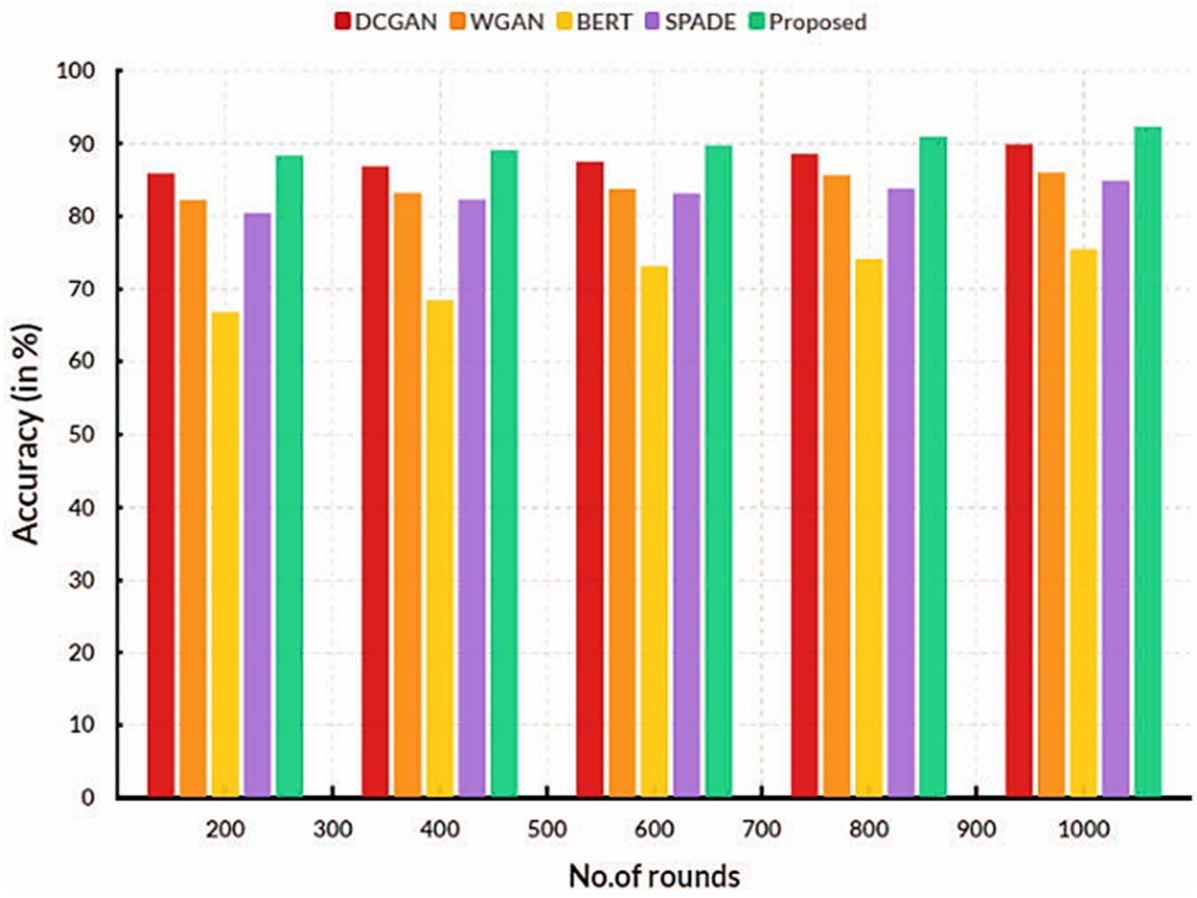



Figure 17: Comparison of Accuracy

Additionally, generative AI allows organizations to preemptively detect threats before they occur, as it is able to identify behaviors which could possibly indicate malicious activity. This tool allows organizations to be more proactive in their approach to cyber security, rather than just passively monitoring their systems. Performance analysis of generative AI can be done to determine its effectiveness in improving an organization's threat intelligence and security measures. This can be done by evaluating factors such as detection latency, accuracy, scalability, and customizability. The lower the detection latency, the faster an organization is able to detect threats.

*B. Evaluation of False positive rate*

Generative AI is the use of AI to create new, unique, and useful data from existing data, rather than simply transforming existing data into potentially useful forms. Generative AI is becoming increasingly important in enhancing cyber security measures, and is playing a major role in the development of improved threat intelligence solutions. Generative AI can be used to generate realistic threat models which can be used to assess and evaluate potential security risks. By leveraging comprehensive data sets, generative AI models can create multiple, virtual simulations of real-world threats. Table 2 given the comparison of various algorithm for false positive rate.

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 |

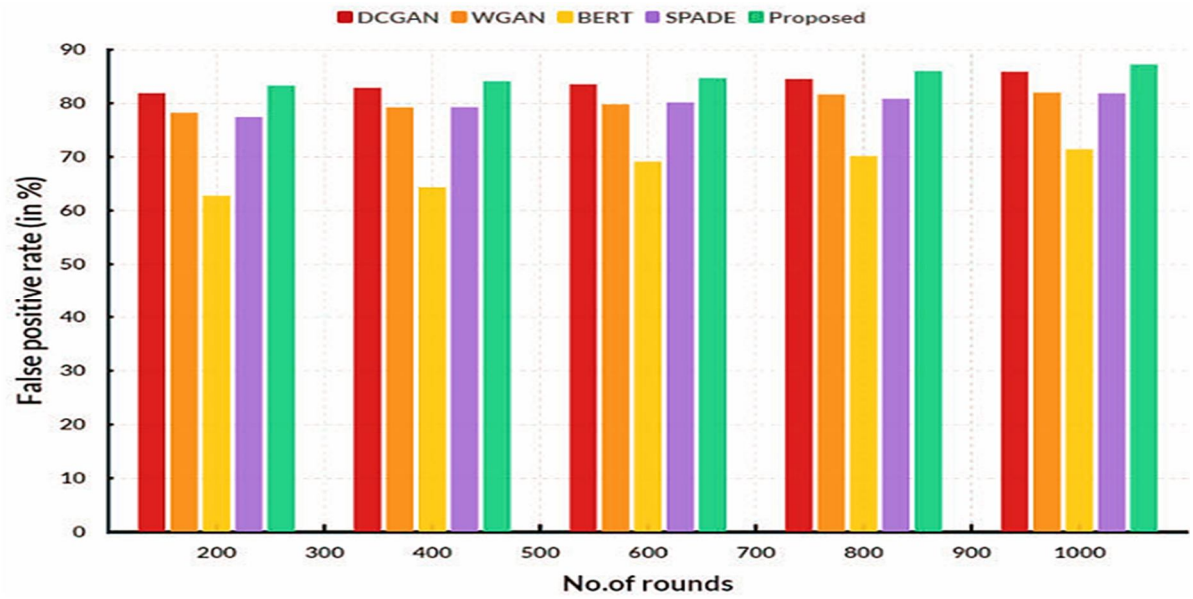



Figure 18: Comparison of false positive rate

These simulations can be used to gain insights from various scenarios in order to develop efficient countermeasures. Generative AI can also be used to identify and analyze large volumes of structured and unstructured data to detect potential anomalous activities, such as malicious activity. By mimicking human behavior, generative AI models can detect patterns and anomalies in data that would be difficult or impossible to detect using traditional security solutions. This can lead to improved threat detection, allowing organizations to effectively respond to threats before they become serious attacks.

*C. Evaluation of False negative rate*

The use of AI and machine learning for threat intelligence and cyber security measures is becoming increasingly popular. As the sophistication of threats continues to increase, AI is

proving to be an effective tool for helping to detect and prevent malicious activity. Generative AI, in particular, is being used in various ways to enhance security measures. Generative AI can be used to identify emerging threats in real-time. Table 3 given the comparison of various algorithm for false negative rate.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

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 |

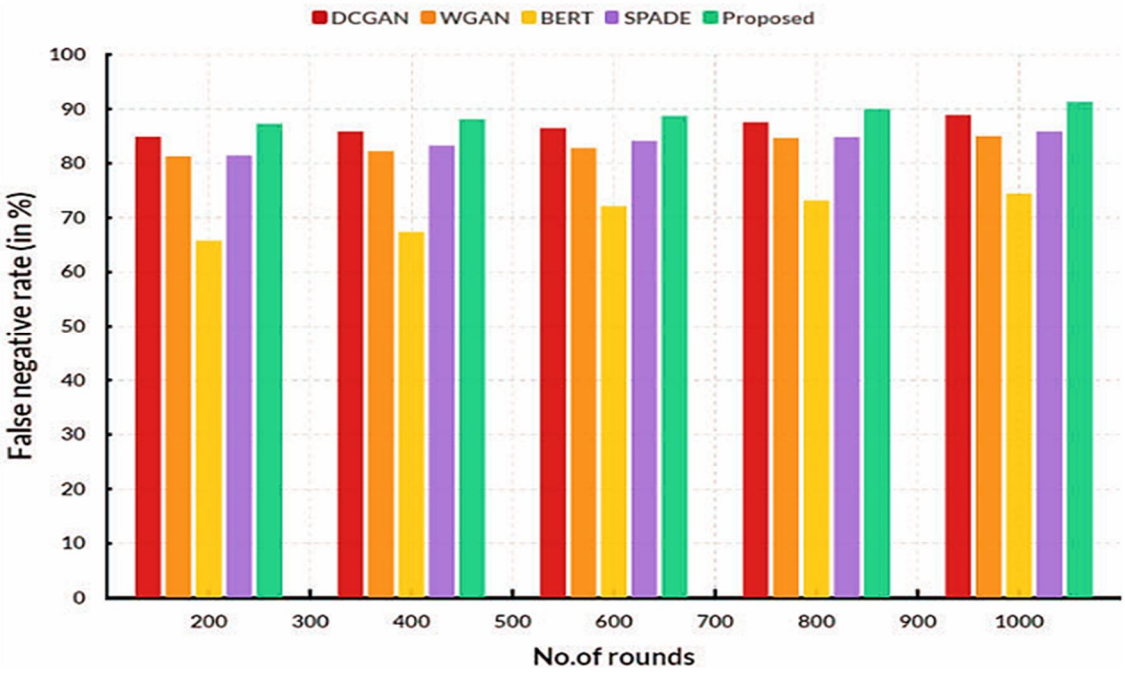



Figure 19: Comparison of false negative rate

This helps to detect malicious activity which may be missed by traditional security solutions. Additionally, it can be used to analyze user activity across various systems to detect patterns that may indicate malicious activity or a breach. Generative AI can also be used to generate "what-if" scenarios or simulations in order to simulate a potential attack and its potential damage in order to design more secure systems. Generative AI can also be used to automate security measures in order to reduce the amount of time and resources it takes to maintain secure systems. Additionally, AI can be used to identify and highlight suspicious activity that may be missed by humans. Finally, generative AI can be used to continuously monitor and update security systems in order to stay ahead of potential threats.

*D. Evaluation of Response time*

Generative AI is a type of artificial intelligence that has the ability to autonomously learn from datasets to generate new, previously unseen data. It can be used to help improve threat intelligence and cyber security measures by detecting threats before they become dangerous or damaging. Generative AI can be used to rapidly identify anomalies in data, and alert security personnel when a threat is detected. This can enable faster response times and better overall protection from cyber-attacks. Table 4 given the comparison of various algorithm for response 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 |

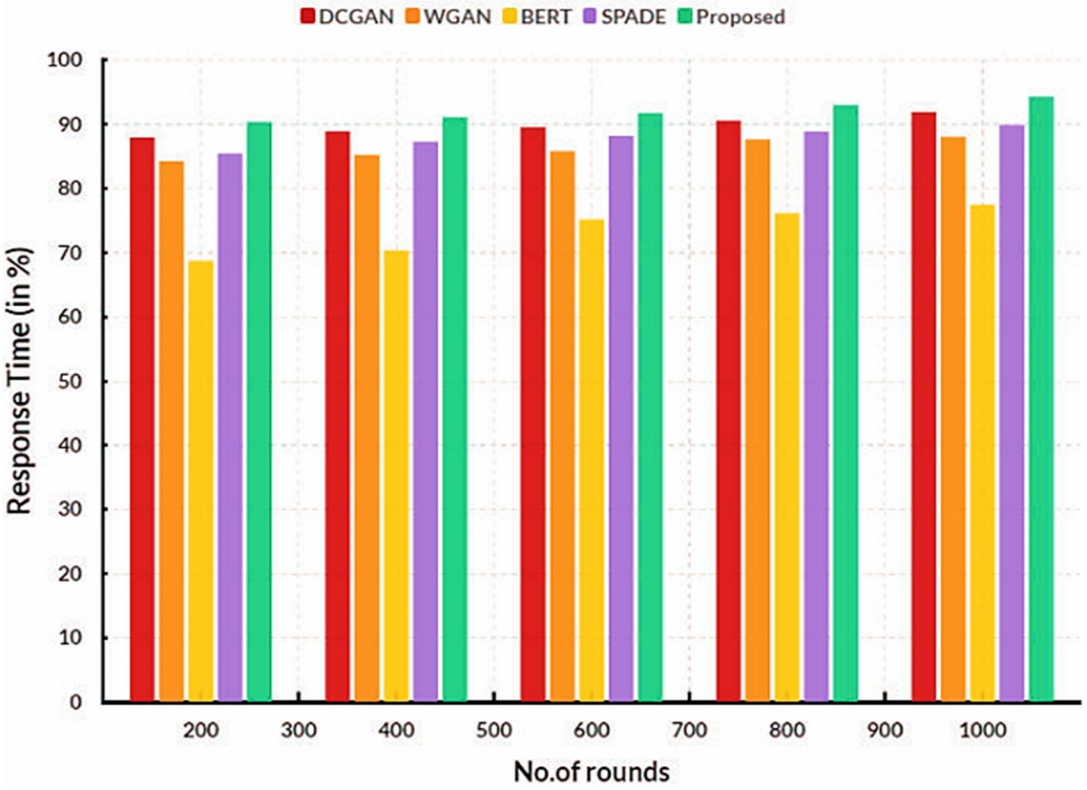



Figure 20: Comparison of response time

Generative AI can also be used to create simulations that allow security professionals to practice responding to potential security threats by replicating real-world scenarios. This can help to identify potential vulnerabilities and improve the effectiveness of security measures. Finally, generative AI can be used to detect and block malicious software and other threats, helping to prevent damage from occurring due to newly developed threats. Overall, generative AI can be a powerful tool to enhance threat intelligence and cyber security measures. Generative AI can help organizations quickly identify malicious threats and react to them in the most effective way possible. This information can then be used to adjust existing cyber defence measures and help organizations stay one step ahead of potential threats. Generative AI can also detect vulnerabilities in existing systems and networks, helping to patch and protect them in the most efficient way possible. The use of generative AI in threat intelligence and cyber security solutions can help organizations stay safe, prevent cyber-attacks, detect them quickly, and respond effectively.

## VII. SECTION IV

CONCLUSION

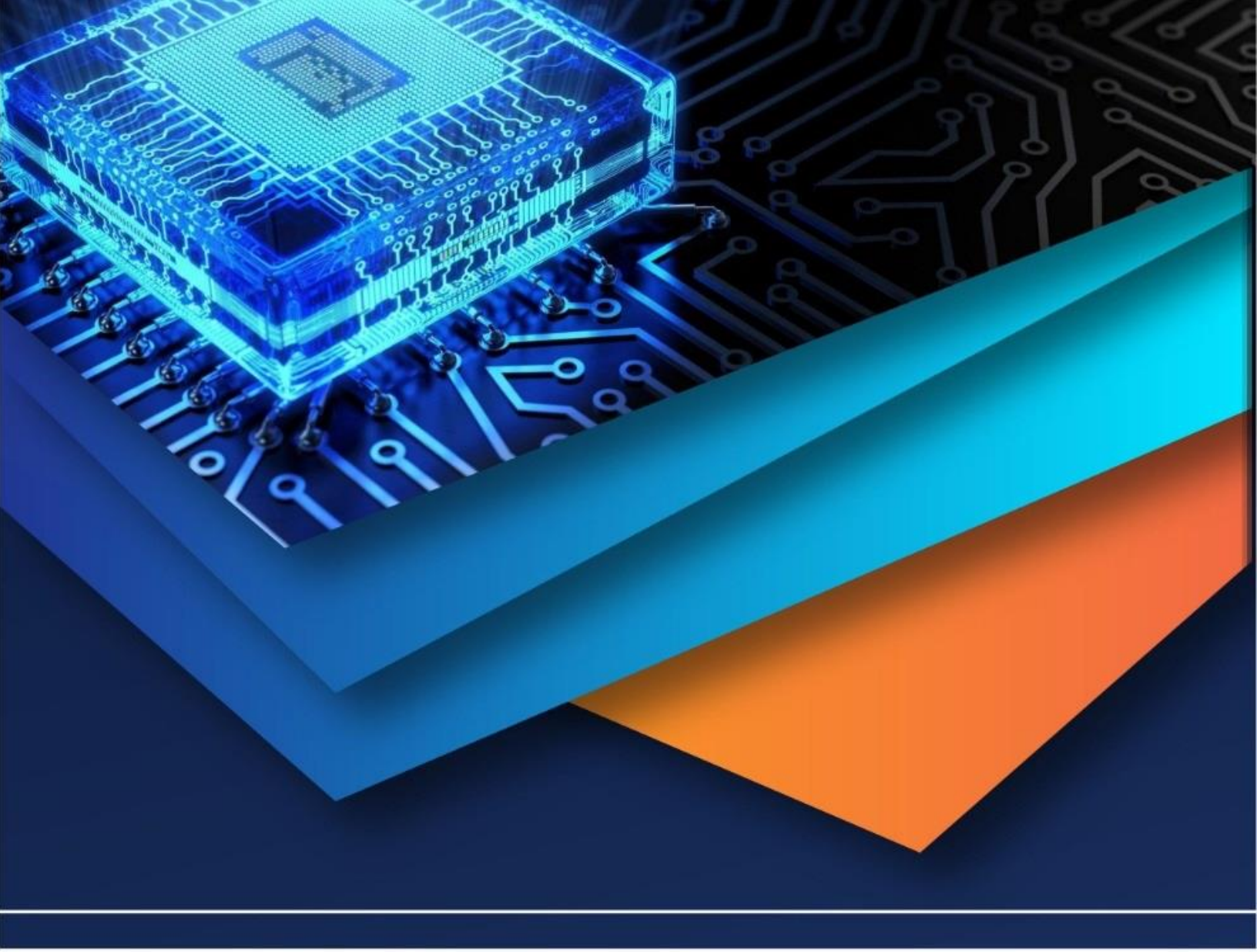
Generative AI has been demonstrated to be an effective tool for enhancing threat intelligence and cyber security measures. Generative AI can be used to automatically generate datasets to train Machine Learning algorithms, as well as data augmentation and reinforcement learning algorithms to better detect anomalous or malicious activity.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Additionally, it can be used to identify patterns in previously unclassified data, thereby increasing the accuracy of threat detection. Additionally, Generative AI can be used to improve the effectiveness of existing cyber security systems. Due to its potential to improve threat intelligence and cyber security measures, generative AI is emerging as an important tool for the future of cyber security. This type of AI can generate both positive and negative threat information, can detect shifting trends and patterns, and can even simulate malicious actors. It can also be used to produce false positives and negatives on a large scale, so that networks can be better prepared and protected from any potential or existing threats. AI-based solutions can also dynamically adjust the response time of the threat intelligence and the response measures to ensure a better response and more effective countermeasures. Generative AI can also help to protect against malicious activities and attempts. Its ability to identify relationships between datasets and detect patterns can help flag potential malicious activities or those that are associated with suspicious entities.

In essence, the proposed improvements serve as a comprehensive strategy for advancing AI-based firewalls into the next generation of cybersecurity. The synergistic integration of interpretability, adaptability, scalability, resilience against adversarial attacks, human-centric features, and regulatory compliance measures can collectively elevate the effectiveness and trustworthiness of these cybersecurity solutions. As the cybersecurity landscape continues to evolve, these proposed improvements position AI-based firewalls as adaptive, robust, and ethical defenders against an ever-expanding array of cyber threats.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)