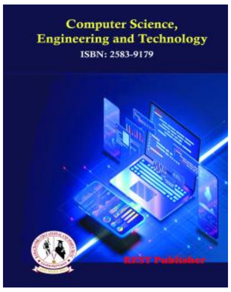
Computer Science, Engineering and Technology

Vol: 3(2), June 2025

REST Publisher; ISSN: 2583-9179 (Online)

Website: https://restpublisher.com/journals/cset/

DOI: https://doi.org/10.46632/cset/3/2/2



Enhancing Cybersecurity with AI: Insights from Grey Relational Analysis

[*]Madhusudhan Dasari Sreeramulu

Leading financial institution USA

**Corresponding Author Email: Dsmadhu007@gmail.com*

Abstract: *Artificial Intelligence (AI) is revolutionizing cybersecurity by improving threat identification, mitigation, and protection strategies. As cyber threats become more complex and sophisticated, AI-driven solutions play a key role in strengthening the security architecture and ensuring proactive protection, AI-driven solutions offer proactive defense strategies, real-time network monitoring, and automated security protocols. This research employs the The Gray Correlation Analysis (GRA) method is used to evaluate the performance of AI in five important domains: communication protocols (C1), node security (C2), network monitoring (C3), cryptography (C4), and security policy (C5). study highlights how AI optimizes security frameworks, mitigates cyber risks, and strengthens overall defense mechanisms. The results indicate that AI significantly improves cybersecurity resilience by addressing vulnerabilities across multiple layers of security. Research Significance: Cyber threats are evolving, requiring intelligent and adaptive security measures AI enhances conventional cybersecurity approaches by automating threat detection and mitigation. Assessing the impact of AI on the security architecture helps improve security mechanisms and response effectiveness. impact on key security components provides insights into its effectiveness. Methodology: Grey Relational Analysis (GRA) Grey Relational Analysis (GRA) is used to assess the relationship between multiple security factors in AI-driven cybersecurity. GRA helps in ranking and determining the most effective AI applications in cybersecurity by analyzing Communication Protocols (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). Alternative Approaches: Communication Protocol (C1): AI-based secure communication frameworks and anomaly detection in data exchange. Node Security (C2): AI-driven authentication, endpoint protection, and intrusion detection at the node level. Network Monitoring (C3): AI-powered network traffic analysis, anomaly detection, and automated threat response. Cryptography (C4): AI-assisted encryption, quantum-resistant algorithms, and secure key management. Security Policy (C5): AI-enhanced policy enforcement, adaptive security frameworks, and compliance monitoring. Evaluation Parameters: Threat Intelligence AI analyzes vast datasets to predict, dentify, analyze, and neutralize cyber threats by recognizing attack patterns and vulnerabilities before exploitation. Intrusion Detection and Prevention AI enhances Intrusion Detection Systems (IDS) and Through Intrusion Prevention Methods (IPM) identifying malicious activities and blocking attacks proactively. Malware Detection and Analysis AI-powered cybersecurity solutions detect, classify, and neutralize malware using machine learning algorithms and behavioral analysis. User and Entity Behavior Analytics (UEBA) AI monitors Monitor user behavior to identify abuse, prevent unauthorized access, and detect insider threats enhancing cybersecurity posture. Automated Incident Response AI accelerates cybersecurity responses by automating threat mitigation, reducing human intervention, and minimizing damage from cyberattacks. Results: The study findings indicate that AI significantly improves cybersecurity across all parameters. AI-driven network monitoring (C3) and cryptography (C4) exhibit the highest impact in mitigating threats. Node security (C2) and communication protocols (C1) demonstrate enhanced efficiency in securing endpoints and data exchange. Security policies (C5) benefit from AI-driven automation, ensuring compliance and real-time adaptation to threats. The GRA analysis highlights AI plays a key role in improving cybersecurity resilience and reducing the likelihood of cyber threats attacks.*

Keywords: *Artificial Intelligence in Cybersecurity, AI-driven Threat Detection, Grey Relational Analysis (GRA), Network Security Automation, AI-powered Cryptography, Intrusion Detection Systems (IDS), Anomaly Detection in Cybersecurity, AI-enhanced Security Policies*

1. INTRODUCTION

Attacks on organizations have become increasingly dangerous as attackers expand their expertise in finding vulnerabilities in cybersecurity technologies. Incorporating artificial intelligence into cybersecurity helps prevent errors, which is Among the main advantages of AI in improving security measures. It has been demonstrated that systems can adapt and learn from a variety of factors, contributing to the technology's significant relevance in cybersecurity. While artificial intelligence offers benefits in cybersecurity, it comes with some limitations that affect its effectiveness. The limitations highlight how individuals use AI for their own benefit, which leads to challenges in cybersecurity. Researchers and innovators should strive to address and mitigate these barriers.[1] This advancement is leading The incidence, scale, and severity of cyber-attacks have led to an increase, highlighting the importance of intelligence-led cybersecurity measures to provide adaptive security mechanisms and effectively manage large volumes of data. AI is becoming an integral part of cybersecurity, being AI is becoming essential, being utilized in numerous applications to support and expedite security procedures human security teams. The evolving cybersecurity landscape, with increasing interest from researchers in both AI and cybersecurity, underscores its growing importance, is fueling further advancements in the field. The choice of These two levels seek to create an understandable and straightforward taxonomy of the body of research on artificial intelligence in cybersecurity, guaranteeing the correct classification of solutions. In addition, the proposed taxonomy defines AI-driven applications can be applied to various levels of the cybersecurity framework introducing a third level that joins the first two.[2]Here, we define these categories and provide references to their specific applications in cybersecurity. However, our focus is not on discussing natural language processing, artificial intelligence, or computer vision, as we consider those to be specialized AI applications. This highlights the challenge of obtaining the information needed to build real-world applications. An example of a cybersecurity expert system designed to assist in security planning, selection of security measures, and optimization of resource allocation. Early research has also explored the use of expert systems for intrusion detection. For the advancement of When using AI techniques in cybersecurity, it's important to differentiate between short-term goals and long-term plans. Numerous AI methodologies can be directly applied to cybersecurity, and certain security issues call for more sophisticated and superior solutions than those currently in place. A review of publications indicates that the most commonly used AI advances in cybersecurity stem from research on artificial neural networks. The use of Neural networks are an important part of cybersecurity. However, there is a critical need to implement intelligent cybersecurity methods in various areas where neural networks are not the most suitable technology.[4] This article aims to conduct a systematic literature review to identify studies on AI-driven cyberattacks and assess their relevance and applicability to c Cybersecurity. With the rise of digital transformation, machine learning plays a key role in cybersecurity research powered by AI. Specifically, AI—particularly machine learning—is being applied to security tactics as well as cyberattacks. This report emphasizes the vulnerabilities in IoT devices inside Industry 4.0, underscoring the significance of cybersecurity in the Fourth Industrial Revolution. The writers investigate how blockchain technology can be used. as a potential solution to address the cybersecurity challenges associated with these vulnerabilities. This study Highlights the importance of cybersecurity infrastructure and explores strategies for assessing, preventing, and addressing cyber threats in industrial cyber-physical systems. The research results indicate that the proposed model performed better than other machine learning models available on the market in a real cybersecurity scenario involving IoT devices within Industry 4.0.[5] Artificial neural networks, a key AI technique, laid the foundation for modern research in cloud cybersecurity. Current research areas, including deep neural networks for facial recognition and speech recognition, have the potential to drive future advances in emerging technologies, especially AI-driven security systems. This article explores data mining, machine learning tools, and techniques used in AI applications for cybersecurity. It helps users effectively test and compare various machine learning techniques on new datasets, primarily focusing on AI applications in cybersecurity. In addition, this article serves as a key reference in the field of AI-driven cybersecurity. These were displayed through a unified user interface to illustrate the distribution of fields related to AI applications in cybersecurity. The number preceding each journal indicates the number of papers published on AI applications in cybersecurity. In the overlay map, weak arc connections or thick lane curves in different colors illustrate the connections and interactions between journals and disciplines.[6] AI-driven cybersecurity solutions struggle to explain their effects— From identification and prediction to analysis and strategic decision making in a way that is easily understandable to humans. The researchers propose that improving AI interpretation can help select Effective anonymization methods for machine learning algorithms can help identify and assess potential biases when interpreting ML results. From a cybersecurity perspective, most studies emphasize intrusion detection systems and their applications in known use cases. However, the cybersecurity discussions in that book do not delve deeply into the technical aspects, leaving out many implementation details and technical considerations innovations. This survey explores the use of description and identifies the methods most appropriate for cybersecurity use cases. This discussion includes explanations for cybersecurity, emphasizing the need to effectively capture changes in attacker strategy.[7] AI's primary benefits may lie not only in reducing electricity, water, and land use, but also in its ability to promote and improve more effective environmental management. To gain insight into the U.S. government's cybersecurity plans, the researchers are also examining Department of Homeland Security's Cybersecurity Policies coming years. Their findings suggest that blockchain technology will have significant audit implications, leading to significant changes in the sector. This research study focuses on improving cybersecurity through semantic web technologies. A framework for automatically extracting and analyzing online material is put out by the authors. using semantic web technologies. The model processes and analyzes online resources using parts of natural ontological language relevant to cybersecurity as input data. a thorough national cybersecurity framework that offers helpful recommendations for choosing and putting into place efficient cybersecurity measures. To develop an intelligent and automated security architecture, analyze cybersecurity data to identify patterns or insights and build a data-driven model accordingly.[8] Cybersecurity presents many challenges and performance barriers, making it difficult for organizations to effectively address them. This report explores key best practices and effective strategies for combating Establishing a secure digital environment that prevents cybercrime and facilitates secure data transfer between electronic devices free of malicious software. Key cybersecurity measures to protect the digital environment will be examined, including strategies to prevent computers from being compromised or manipulated. Cybersecurity focuses Focusing on protecting software and applications from vulnerabilities that serve as key entry points for cyberattacks. The shortage of cybersecurity professionals is one of the biggest challenges facing organizations, as a sufficient number of experts in this field are needed to create a secure digital environment. Cybercriminals exploit these weaknesses in information systems for hacking purposes by studying computer procedures and user behavior. Cybersecurity plays a key role in creating a secure digital environment by eliminating vulnerabilities and preventing unauthorized access.[9] The field of AI in cybersecurity is still in its infancy. This article seeks to advance the discipline by providing a foundation for moving forward. It begins with an overview of existing cybersecurity data, summarizes current AI applications in cybersecurity, and highlights key limitations in the field. Based on these challenges, the article proposes a multidisciplinary roadmap that focuses on critical areas Cybersecurity applications and data, including cutting-edge AI techniques and AI-powered decision-making The diverse, complex, and rapidly changing nature of both AI and cybersecurity will slow the field's progress. AI combines concepts Combining insights from mathematics, biology, and other fields, a comprehensive understanding of cybersecurity protocols, risks, and security strategies is essential. Our aim is to provide a structured overview of fundamental cybersecurity data, current AI-driven cybersecurity applications, and key limitations within the existing framework.[10] By increasing the effectiveness and precision of threat detection, artificial intelligence (AI) in cybersecurity aids in adapting to the always changing landscape of cyberthreats. While human involvement in cybersecurity remains essential, many network security processes will be automated and managed by AI. Artificial Intelligence (AI) serves as a valuable asset for cybersecurity teams, improving security protection against various threats and cyberattacks. The assessment emphasizes future research opportunities in data representation, advanced AI techniques, emerging cybersecurity applications, and the development of innovative infrastructures. This section explores practical applications Use artificial intelligence (AI) in cybersecurity, which includes utilizing AI tools to defend data and digital systems from online attacks and unauthorized access.[11] Human errors are intentional and often malicious, whereas cybersecurity errors are usually Incidentally. The domain Modern network and systems security primarily prioritizes avoiding cybersecurity mistakes instead of detecting or explaining them. The initial step was to identify key research categories on interpretation in artificial intelligence and cybersecurity. The survey explores the techniques and approaches needed to incorporate description into cybersecurity applications.[12] This underscores the need for extensive Non-technical elements that may impact AI-driven threats are taken into account in cybersecurity research on AI. A thorough categorization of AI-driven hacks has been developed thanks to research in this area. The motivations of AI-based attackers are also examined, as well as new developments in defensive AI tactics. AI is a flexible instrument that may be used for both offensive and defensive cybersecurity operations.[13] Artificial Intelligence (AI) in cybersecurity, supported by machine learning, is emerging as a useful tool for the future. Compared to other industries, human involvement in cybersecurity is important and essential. While the industry still relies heavily on human input, technological advancements are steadily improving efficiency in specific tasks. Cybersecurity challenges have increased significantly. This essay aims to provide a thorough summary of various AI applications and explores how AI systems can help organizations combat everyday cyber threats.[14] Conventional cybersecurity solutions are increasingly inadequate at detecting and preventing new cyber threats. A rapidly growing and increasingly complex threat is the zero-day attack, which cybersecurity experts and software or hardware developers are unaware of until it is exploited. We highlight several key challenges facing the cybersecurity community that need to be addressed moving forward.[15]

2. MATERIALS AND METHOD

Alternatives: Communication Protocol (C1): Communication protocols are essential for secure data exchange between computers and devices. AI improves Cybersecurity by detecting weaknesses in communication protocols and preventing unauthorized access or data breaches. Machine learning algorithms evaluate network traffic patterns, identify anomalies, and mitigate cyber threats such as man-in-the-middle attacks. Through automation, threat detection, AI helps secure communication channels and ensure data integrity. Endpoint Security (C2): Endpoint security is dedicated to protecting individual devices within the network. AI-powered security solutions can monitor and evaluate each endpoint for potential vulnerabilities, unauthorized access, and malicious activity. Through behavioral analysis and anomaly detection, AI can identify compromised nodes and take corrective actions to prevent network breaches. This proactive approach strengthens endpoint security and reduces the risk of cyberattacks. Network Monitoring (C3): Network monitoring plays a key role in detecting potential cyber Threats immediately. AI-powered tools process large amounts of network data, detect unusual behavior, and block cyber intrusions. Unlike conventional approaches, AI can detect complex threats, including zero-day attacks and advanced persistent threats (APTs) by recognizing deviations from normal behavior. Automated AI-driven monitoring improves cybersecurity by providing rapid threat detection and response.Cryptography (C4): Cryptography is the foundation of protecting sensitive data through encryption and decryption techniques. AI improves cryptographic security, creates stronger encryption algorithms, and finds weaknesses in existing cryptographic methods. In addition, AI helps automate encryption key management and prevent cryptographic attacks such as brute force and side-channel attacks. By integrating AI with cryptography, organizations can strengthen data security and protect sensitive information from cyber threats. Security Policy (C5): A strong security policy is essential to maintaining cybersecurity standards within an organization. AI helps enforce security policies by continuously monitoring compliance and detecting breaches. AI-powered security architectures can adapt to evolving threats, ensuring organizations follow best security practices. By analyzing past incidents and predicting future risks, AI helps create dynamic and effective security policies that evolve with the cybersecurity landscape.

Evaluation parameter: Threat Intelligence AI-powered Threat Intelligence enhances cybersecurity by analyzing vast datasets to identify attack patterns, vulnerabilities, and emerging cyber threats. Machine learning algorithms process real-time threat feeds, enabling proactive defense mechanisms. AI continuously refines threat detection models, helping organizations predict, prevent, and respond to cyberattacks before they escalate. Intrusion Detection and Prevention AI-driven Intrusion Detection and Prevention Systems (IDPS) monitor network activity to identify malicious behavior and unauthorized access attempts. By leveraging machine learning, these systems detect zero-day attacks and anomalous patterns, improving response time. AI enhances traditional IDPS by reducing false positives and automating threat mitigation, strengthening overall network security. Malware Detection and Analysis AI revolutionizes Malware Detection and Analysis by identifying, classifying, and neutralizing malware using deep learning and behavioral analysis. Unlike signature-based detection, AI detects polymorphic and zero-day malware by analyzing execution patterns and system behavior. This proactive approach improves cybersecurity resilience against evolving malware threats. User and Entity Behavior Analytics (UEBA) AI-driven User and Entity Behavior Analytics (UEBA) enhances security by monitoring user activities, device interactions, and network traffic to detect anomalies. By learning normal behavior patterns, AI identifies suspicious deviations, such as insider threats, credential misuse, and lateral movements within a network. UEBA strengthens security by preventing unauthorized access. Automated Incident Response AI-powered Automated Incident Response accelerates threat mitigation by analyzing incidents, prioritizing alerts, and executing predefined security actions. AI-driven automation reduces response time, minimizes human intervention, and prevents cyberattacks from spreading. By integrating AI with Security Orchestration, Automation, and Response (SOAR) systems, organizations achieve faster and more efficient cybersecurity operations.

GRA

GRA models, initially based on proximity, combine both similarity and proximity, and extend from analyzing relationships between curves to curved surfaces, three-dimensional spaces, and surfaces in n-dimensional spaces. Further exploration of GRA models is encouraged, especially to understand their characteristics, their role, applicability, and modeling requirements. Early GRA models relied on specific relationship coefficients, whereas modern models adopt a holistic approach, emphasizing similarity and comprehensive analysis. A key aspect of supply chain flexibility includes minimizing supplier vulnerabilities, understanding risks, and following proper protocols. This process applies to first- and second-tier suppliers, where a gray relative grade is calculated for each tier. The final gray relative grade is determined by multiplying the average gray relative grades of successive tiers. The normalization process of GRA is more straightforward and logical than the fuzzy TOPSIS method, providing clear distinctions between alternatives by providing significant variations in the grade values. The IHGRA method addresses the previous limitations of GRA by incorporating goal-based criteria, and adapts the green regression supplier evaluation model for broader decision-making applications. The proposed GRA module is lightweight and flexible, seamlessly integrating with adaptive neural networks to improve performance. The key features of this module include group-wise rotation and group-wise focus. The group-wise rotation module uses an angle generator to predict multiple rotation angles from input features. This interaction in the GRA module facilitates feature extraction from multiple perspectives. Unlike resource-intensive training methods, this approach uses pre-trained ResNet weights, focusing on training only newly added GRA modules.Penta-partitioned neutrosophic sets provide a robust mathematical framework for addressing incomplete, ambiguous, and inconsistent information. The research strengthens decision-making under uncertainty by extending The GRA method, rooted in geometric mathematics, adheres to a combination of multiple criteria decision making (MCDM) methods, such as the Fuzzy Analytic Hierarchy Process (FAHP) and GRA Relational Analysis (GRA), has proven effective in personnel selection. FAHP determines the importance weights of personnel based on the criteria, which are then decomposed using the centroid method. The Gray Correlation Coefficient (GRC) establishes the relationships Between expected and observed experimental data with Gray relational grade. (GRG) is calculated to evaluate the output responses. A study on agricultural machinery confirmed the feasibility of this model. A comparison of ranking results using GRA-TOPSIS, GRA, and TOPSIS methods demonstrated the advantages of GRA-TOPSIS in evaluation accuracy. Traditional GRA models assume equal attribute weights, which limits their effectiveness in hierarchical structures. which is preferred for measuring supply chain complexity due to its ability to combine interdependent factors into a unified mathematical framework. The PSO-GRA-BPNN model GRA has also been used for pricing models, especially for low-cost used cars, rather than the BPNN and GRA-BPNN models. As a method rooted in gray system theory, GRA is widely used in industrial optimization, providing solutions to uncertainty and complex multi-response interactions. In manufacturing, GRA determines the relationships between machine parameters and performance, using discrete measurement techniques to handle uncertainty more effectively than conventional mathematical analysis. Feature extraction and classification also benefit from GRA, as extracted features are classified based on their corresponding gray levels. The method accommodates a variety of training-test partitions, ensuring applicability across a variety of applications.

3. RESULTS AND DISCUSSION

TABLE 1. Cybersecurity with AI

	Threat Intelligence	Intrusion Detection and Prevention	Malware Detection and Analysis	User and Entity Behavior Analytics (UEBA)	Automated Incident Response
Communication protocol (C1)	230.00	365.00	560.00	220.00	354.00
node security (C2	324.00	451.00	245.00	230.00	265.00
network monitoring (C3)	654.00	265.00	250.00	240.00	452.00
cryptography (C4)	257.00	245.00	354.00	256.00	365.00
security policy (C5)	356.00	354.00	200.00	245.00	254.00

Artificial Intelligence (AI) plays a vital role in cybersecurity by enhancing Threat Intelligence, Intrusion Detection and Prevention, Malware Detection and Analysis, User and Entity Behavior Analytics (UEBA), and Automated Incident Response. The evaluation of AI's impact on these security domains is based on key parameters: Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). For Threat Intelligence, Network Monitoring (C3) (654.00) has the highest impact, indicating AI’s ability to analyze and detect cyber threats in real time. Node Security (C2) (324.00) and Security Policy (C5) (356.00) also contribute significantly. Intrusion Detection and Prevention (IDPS) relies heavily on Node Security (C2) (451.00) and Communication Protocol (C1) (365.00), proving AI's efficiency in detecting and mitigating cyber intrusions. In Malware Detection and Analysis, Communication Protocol (C1) (560.00) plays the most crucial role, showing AI’s strength in analyzing network traffic to identify malware. Cryptography (C4) (354.00) also helps secure data. For UEBA, Communication Protocol (C1) (220.00) and Network Monitoring (C3) (240.00) highlight AI’s ability to track suspicious behavior.

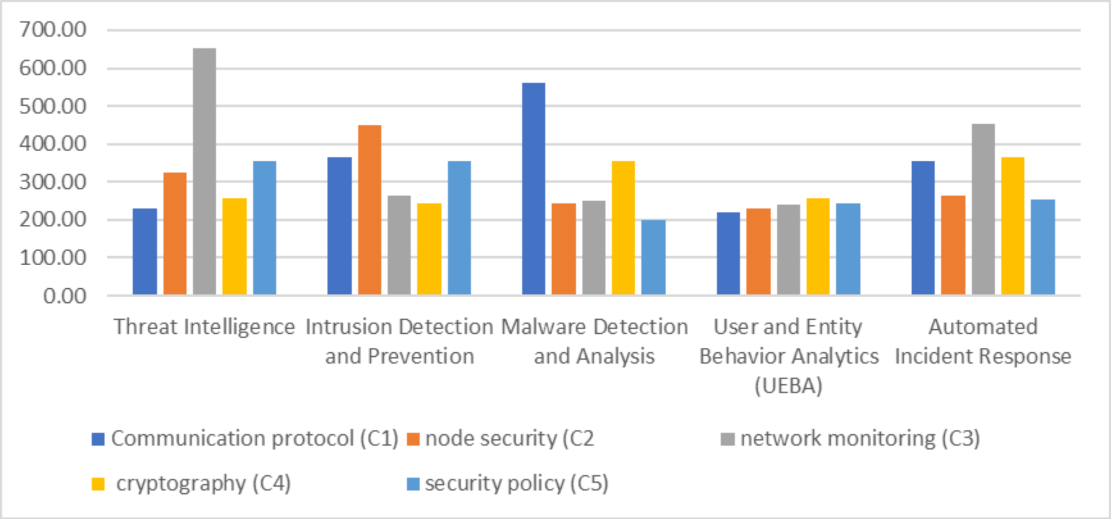


FIGURE 1. Cybersecurity with AI

Figure 1 illustrates the impact of Artificial Intelligence (AI) on various cybersecurity domains, including Threat Intelligence, Intrusion Detection and Prevention, Malware Detection and Analysis, User and Entity Behavior Analytics (UEBA), and Automated Incident Response. The evaluation considers five key security parameters: Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). The chart reveals significant variations in the effectiveness of these parameters across different cybersecurity applications. For instance, network monitoring (C3) exhibits the highest value in Threat Intelligence, while communication protocol (C1) dominates Malware Detection and Analysis. Cryptography (C4) and security policy (C5) contribute consistently across multiple domains, ensuring data protection and regulatory compliance. This analysis underscores the critical role of AI in optimizing cybersecurity measures, providing deeper insights into threat mitigation and response strategies.

TABLE 2. Normalized Data

	Threat Intelligence	Intrusion Detection and Prevention	Malware Detection and Analysis	User and Entity Behavior Analytics (UEBA)	Automated Incident Response
Communication protocol (C1)	0.0000	0.5825	1.0000	1.0000	0.4949
node security (C2	0.2217	1.0000	0.1250	0.7222	0.9444
network monitoring (C3)	1.0000	0.0971	0.1389	0.4444	0.0000
cryptography (C4)	0.0637	0.0000	0.4278	0.0000	0.4394
security policy (C5)	0.2972	0.5291	0.0000	0.3056	1.0000

Artificial Intelligence (AI) significantly enhances cybersecurity through its application in Threat Intelligence, Intrusion Detection and Prevention, Malware Detection and Analysis, User and Entity Behavior Analytics (UEBA), and Automated Incident Response. The effectiveness of these security domains is evaluated based on Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). For Threat Intelligence, Network Monitoring (C3) (1.0000) has the highest impact, indicating AI's ability to analyze large-scale network activity for threat detection. Node Security (C2) (0.2217) and Security Policy (C5) (0.2972) also contribute, showing AI's role in protecting individual devices and enforcing security policies. Intrusion Detection and Prevention is most influenced by Node Security (C2) (1.0000) and Communication Protocol (C1) (0.5825), demonstrating AI's efficiency in detecting and blocking cyber intrusions. In Malware Detection and Analysis, Communication Protocol (C1) (1.0000) plays a crucial role, highlighting AI's capability to analyze network traffic and detect malware threats. Cryptography (C4) (0.4278) also contributes by ensuring secure data handling. For UEBA, Communication Protocol (C1) (1.0000) and Node Security (C2) (0.7222) emphasize AI's ability to monitor user behavior and prevent unauthorized access.

TABLE 3. Deviation sequence

	Threat Intelligence	Intrusion Detection and Prevention	Malware Detection and Analysis	User and Entity Behavior Analytics (UEBA)	Automated Incident Response
Communication protocol (C1)	1.0000	0.4175	0.0000	0.0000	0.5051
node security (C2	0.7783	0.0000	0.8750	0.2778	0.0556
network monitoring (C3)	0.0000	0.9029	0.8611	0.5556	1.0000
cryptography (C4)	0.9363	1.0000	0.5722	1.0000	0.5606
security policy (C5)	0.7028	0.4709	1.0000	0.6944	0.0000

Artificial Intelligence (AI) significantly enhances cybersecurity through its impact on Threat Intelligence, Intrusion Detection and Prevention, Malware Detection and Analysis, User and Entity Behavior Analytics (UEBA), and Automated Incident Response. The effectiveness of AI in these areas is evaluated based on Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). For Threat Intelligence, Communication Protocol (C1) (1.0000) has the highest impact, highlighting AI's role in securing data transmission and preventing unauthorized access. Cryptography (C4) (0.9363) also contributes significantly, emphasizing AI's ability to strengthen encryption techniques and protect sensitive data. Node Security (C2) (0.7783) and Security Policy (C5) (0.7028) further support AI-driven intelligence gathering by reinforcing endpoint security and compliance measures. In Intrusion Detection and Prevention, Cryptography (C4) (1.0000) and Network Monitoring (C3) (0.9029) play crucial roles, showing AI's effectiveness in detecting threats through encrypted traffic analysis and real-time network monitoring. Malware Detection and Analysis benefits most from Security Policy (C5) (1.0000) and Node Security (C2) (0.8750), indicating that AI enhances policy enforcement and endpoint protection against malware attacks. For UEBA, Cryptography (C4) (1.0000) and Network Monitoring (C3) (0.5556) highlight AI's role in identifying abnormal user behavior and potential insider threats. Finally, Automated Incident Response relies most on Network Monitoring (C3) (1.0000) and Communication Protocol (C1) (0.5051), demonstrating AI's ability to automate responses based on real-time threat analysis.

TABLE 4. Grey relation coefficient

	Threat Intelligence	Intrusion Detection and Prevention	Malware Detection and Analysis	User and Entity Behavior Analytics (UEBA)	Automated Incident Response
Communication protocol (C1)	0.3333	0.5450	1.0000	1.0000	0.4975
node security (C2	0.3911	1.0000	0.3636	0.6429	0.9000
network monitoring (C3)	1.0000	0.3564	0.3673	0.4737	0.3333
cryptography (C4)	0.3481	0.3333	0.4663	0.3333	0.4714
security policy (C5)	0.4157	0.5150	0.3333	0.4186	1.0000

Artificial Intelligence (AI) plays a crucial role in strengthening cybersecurity across multiple domains, including Threat Intelligence, Intrusion Detection and Prevention, Malware Detection and Analysis, User and Entity Behavior Analytics (UEBA), and Automated Incident Response. The evaluation of these security aspects is based on key parameters: Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). For Threat Intelligence, Network Monitoring (C3) (1.0000) has the highest impact, indicating that AI-driven monitoring effectively detects and prevents cyber threats. Node Security (C2) (0.3911) and Security Policy (C5) (0.4157) also play a role in securing endpoints and enforcing compliance. Intrusion Detection and Prevention relies most on Node Security (C2) (1.0000) and Communication Protocol (C1) (0.5450), showcasing AI's role in detecting and mitigating intrusions through device security and communication safeguards. For Malware Detection and Analysis, Communication Protocol (C1) (1.0000) has the highest impact, emphasizing AI's ability to analyze and secure data exchanges against malware threats. Cryptography (C4) (0.4663) also plays a significant role in encrypting sensitive data and preventing attacks. In UEBA, Communication Protocol (C1) (1.0000) and Node Security (C2) (0.6429) highlight AI's effectiveness in monitoring user behavior and preventing unauthorized access. Finally, Automated Incident Response benefits most from Security Policy (C5) (1.0000) and Node Security (C2) (0.9000), demonstrating AI's role in automating security policies and ensuring rapid threat mitigation.

TABLE 5. GRG

	GRG
Communication protocol (C1)	0.6752
node security (C2	0.6595
network monitoring (C3)	0.5062
cryptography (C4)	0.3905
security policy (C5)	0.5365

Artificial Intelligence (AI) plays a critical role in enhancing cybersecurity, with various security parameters contributing to its effectiveness. The Grey Relational Grade (GRG) values help determine the significance of different security measures in AI-driven cybersecurity. The key parameters evaluated are Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). Among these, Communication Protocol (C1) (0.6752) holds the highest significance, indicating that AI-driven security mechanisms greatly enhance the protection of data transmission, ensuring secure and efficient communication channels. Node Security (C2) (0.6595) follows closely, emphasizing the importance of AI in safeguarding endpoints and devices from cyber threats, malware, and unauthorized access. Security Policy (C5) (0.5365) also plays a crucial role, reflecting AI's impact on enforcing security guidelines, risk management, and compliance with cybersecurity frameworks. Network Monitoring (C3) (0.5062) highlights AI's effectiveness in real-time threat detection and network traffic analysis, ensuring continuous monitoring of suspicious activities. Lastly, Cryptography (C4) (0.3905) has the lowest GRG value, suggesting that while AI enhances encryption techniques, its impact is relatively lower compared to other security measures. However, cryptographic methods remain essential for securing sensitive data and preventing unauthorized access.

TABLE 6. Rank

	Rank
Communication protocol (C1)	1
node security (C2	2
network monitoring (C3)	4
cryptography (C4)	5
security policy (C5)	3

The ranking of cybersecurity parameters highlights the relative importance of different security measures in AI-driven cybersecurity. The parameters evaluated include Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5). Communication Protocol (C1) is ranked first (1), indicating its critical role in ensuring secure and reliable data transmission. AI enhances communication protocols by detecting and mitigating cyber threats in real-time, preventing unauthorized access, and securing network exchanges. Node Security (C2) is ranked second (2), demonstrating AI's effectiveness in protecting endpoints from malware, unauthorized intrusions, and other cyber threats. Secure device authentication and anomaly detection further strengthen AI-driven node security. Security Policy (C5) holds the third rank (3), emphasizing AI's role in enforcing cybersecurity policies, risk management strategies, and compliance frameworks. AI enhances automated policy implementation, ensuring that security standards are consistently maintained. Network Monitoring (C3) is ranked fourth (4), showing its role in continuous traffic analysis, intrusion detection, and early warning systems. AI-powered monitoring systems help detect and respond to potential threats before they escalate. Finally, Cryptography (C4) ranks fifth (5), suggesting that while encryption remains a fundamental security mechanism, its impact in AI-driven cybersecurity is relatively lower than other measures. AI does enhance cryptographic techniques, but its primary focus lies in securing communication, devices, and network activities.

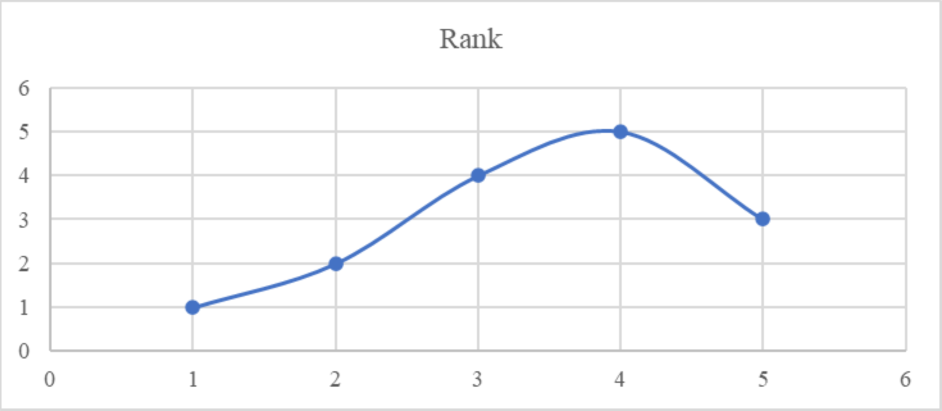


FIGURE 2. Rank

Figure 2 presents the ranking of different security parameters based on the Grey Relational Analysis (GRA) method. The ranking evaluates the effectiveness of AI in cybersecurity across key domains, including Communication Protocol (C1), Node Security (C2), Network Monitoring (C3), Cryptography (C4), and Security Policy (C5).The graph shows a progressive increase in ranking from C1 to C4, with Cryptography (C4) achieving the highest rank. However, the ranking slightly decreases for Security Policy (C5), indicating that while AI plays a crucial role in securing digital infrastructure, its effectiveness varies across different security aspects. This ranking helps in identifying the most influential cybersecurity factors, guiding future AI-driven security enhancements.

4. CONCLUSION

Artificial intelligence (AI) has transformed cybersecurity by improving threat detection, prevention, and response systems. Based on the evaluation of key security parameters— Communication protocols, endpoint security, network monitoring, encryption techniques, and security regulations. it is evident that AI-driven solutions significantly strengthen cyber defense strategies. Communication Protocols and Node Security play the most crucial roles, ensuring secure data exchange and endpoint protection. Security Policies and Network Monitoring further contribute by enforcing compliance and enabling real-time threat detection. While Cryptography remains essential, its impact is comparatively lower in AI-driven cybersecurity frameworks. The ranking analysis highlights that AI is most effective in securing communications, monitoring networks, and automating security policies to mitigate cyber risks. Using machine learning, behavioral analytics, and AI-driven approaches Automated event response helps organizations proactively combat emerging cyber threats. The increasing complexity of cybersecurity challenges AI will remain a key enabler in enhancing security resilience, reducing vulnerabilities, and ensuring a more robust digital infrastructure.

REFERENCES

[1]. Ansari, Meraj Farheen, Bibhu Dash, Pawankumar Sharma, and Nikhitha Yathiraju. "The impact and limitations of artificial intelligence in cybersecurity: a literature review." International Journal of Advanced Research in Computer and Communication Engineering (2022).

[2]. Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. "Artificial intelligence for cybersecurity: Literature review and future research directions." Information Fusion 97 (2023): 101804.

[3]. Zhang, Zhimin, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang, and Kim-Kwang Raymond Choo. "Artificial intelligence in cyber security: research advances, challenges, and opportunities." Artificial Intelligence Review (2022): 1-25.

[4]. De Azambuja, Antonio João Gonçalves, Christian Plesker, Klaus Schützer, Reiner Anderl, Benjamin Schleich, and Vilson Rosa Almeida. "Artificial intelligence-based cyber security in the context of industry 4.0—a survey." Electronics 12, no. 8 (2023): 1920.

[5]. Abbas, Naveed Naeem, Tanveer Ahmed, Syed Habib Ullah Shah, Muhammad Omar, and Han Woo Park. "Investigating the applications of artificial intelligence in cyber security." Scientometrics 121 (2019): 1189-1211.

[6]. Charmet, Fabien, Harry Chandra Tanuwidjaja, Solayman Ayoubi, Pierre-François Gimenez, Yufei Han, Houda Jmila, Gregory Blanc, Takeshi Takahashi, and Zonghua Zhang. "Explainable artificial intelligence for cybersecurity: a literature survey." Annals of Telecommunications 77, no. 11 (2022): 789-812.

[7]. Tao, Feng, Muhammad Shoaib Akhtar, and Zhang Jiayuan. "The future of artificial intelligence in cybersecurity: A comprehensive survey." EAI Endorsed Transactions on Creative Technologies 8, no. 28 (2021).

[8]. Mijwil, Maad M., Mohammad Aljanabi, and ChatGPT ChatGPT. "Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime." Iraqi Journal For Computer Science and Mathematics 4, no. 1 (2023): 8.

[9]. Samtani, Sagar, Murat Kantarcioglu, and Hsinchun Chen. "Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap." ACM Transactions on Management Information Systems (TMIS) 11, no. 4 (2020): 1-19.

[10]. Adewusi, Adebunmi Okechukwu, Ugochukwu Ikechukwu Okoli, Temidayo Olorunsogo, Ejuma Adaga, Donald Obinna Daraojimba, and Ogugua Chimezie Obi. "Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA." World Journal of Advanced Research and Reviews 21, no. 1 (2024): 2263-2275.

[11]. Rjoub, Gaith, Jamal Bentahar, Omar Abdel Wahab, Rabeb Mizouni, Alyssa Song, Robin Cohen, Hadi Otrok, and Azzam Mourad. "A survey on explainable artificial intelligence for cybersecurity." IEEE Transactions on Network and Service Management 20, no. 4 (2023): 5115-5140.

[12]. Malatji, Masike, and Alaa Tolah. "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI." AI and Ethics (2024): 1-28.

[13]. Zhang, Zhimin, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang, and Kim-Kwang Raymond Choo. "Artificial intelligence in cyber security: research advances, challenges, and opportunities." Artificial Intelligence Review (2022): 1-25.

[14]. Zeadally, Sherali, Erwin Adi, Zubair Baig, and Imran A. Khan. "Harnessing artificial intelligence capabilities to improve cybersecurity." Ieee Access 8 (2020): 23817-23837.

[15]. Özdemir, Yavuz, Kemal Gökhan Nalbant, and Hüseyin Başlıgil. "Personnel selection for promotion using an integrated fuzzy analytic hierarchy process-grey relational analysis methodology: a real case study." Anadolu University Journal of Science and Technology A-Applied Sciences and Engineering 19, no. 2 (2018): 278-292.

[16]. Lenzen, Manfred, Richard Wood, and Blanca Gallego. "Some comments on the GRAS method." Economic systems research 19, no. 4 (2007): 461-465.

[17]. Loganathan, D., Shunmugam Satish Kumar, and R. Ramadoss. "Grey relational analysis-based optimisation of input parameters of incremental forming process applied to the AA6061 alloy." Transactions of FAMENA 44, no. 1 (2020): 93-104.

[18]. Lu, Haonan, Yongman Zhao, Xue Zhou, and Zikai Wei. "Selection of agricultural machinery based on improved CRITIC-entropy weight and GRA-TOPSIS method." Processes 10, no. 2 (2022): 266.

[19]. Pakkar, Mohammad Sadegh. "Hierarchy grey relational analysis using DEA and AHP." PSU Research review 1, no. 2 (2017): 150-163.

[20]. Alvarez-Lajonchere, L., N. H. Shoukry, B. Gra, Y. Amador-Cañizares, F. Helle, N. Bedard, I. Guerra et al. "Immunogenicity of CIGB-230, a therapeutic DNA vaccine preparation, in HCV-chronically infected individuals in a Phase I clinical trial." Journal of viral hepatitis 16, no. 3 (2009): 156-167.

[21]. Piya, Sujan, Ahm Shamsuzzoha, Mohammed Khadem, and Mahmoud Al Kindi. "Integrated analytical hierarchy process and grey relational analysis approach to measure supply chain complexity." Benchmarking: An International Journal 28, no. 4 (2021): 1273-1295.

[22]. Liu, Enci, Jie Li, Anni Zheng, Haoran Liu, and Tao Jiang. "Research on the prediction model of the used car price in view of the pso-gra-bp neural network." Sustainability 14, no. 15 (2022): 8993.

[23]. Yaser, EK Mohammed, and K. Shunmugesh. "Multi-objective optimization of milling process parameters in glass fibre reinforced polymer via grey relational analysis and desirability function." Materials Today: Proceedings 11 (2019): 1015-1023.

[24]. Mohamed, Sity Ainy Nor, Edi Syams Zainudin, S. M. Sapuan, Mohd Azaman Md Deros, and AM Tajul Arifin. "Integration of taguchi-grey relational analysis technique in parameter process optimization for rice husk composite." BioResources 14, no. 1 (2019): 1110-1126.

[25]. Das, Suman, Bimal Shil, and Surapati Pramanik. "SVPNS-MADM strategy based on GRA in SVPNS Environment." Neutrosophic Sets and Systems 47, no. 1 (2021): 50-65.