Journal for Technology and Science
Homepage : https://journal.antispublisher.com/index.php/IPTEKS
Email : admin@antispublisher.com

e-ISSN : 3047-4337
JOTECH, Vol. 1, No. 3, July 2024
Page 191-200

Artificial Intelligence Driven Infrastructure Security Enhancing Cybersecurity and Protecting National Security Systems

Chowdhury Amin Abdullah [1], Md Jahidul Islam Ridoy [2]
[1]Seidenberg School of Computer Science and Information systems, Pace University, New York, United States.
[2]Independent Researcher, New York, United States.

DOI : https://doi.org/10.61796/ipteks.v1i3.498

Sections Info

Article history:
Submitted: April 07, 2024
Final Revised: May 26, 2024
Accepted: June 18, 2024
Published: July 25, 2024

Keywords:
Artificial Intelligence
Cybersecurity
National Security
Data Protection
Critical Infrastructure
Machine Learning

ABSTRACT

Objective: *Artificial Intelligence (AI) functions as a fundamental technological solution which defends national security systems through improved cybersecurity infrastructure against sophisticated cyber threats. The fast growth of digital technology has made vital infrastructure systems vulnerable to cyber threats which include phishing attacks and ransomware and malware infections and data breach incidents.* ***Method:*** *The research used a quantitative survey-based design which collected data from 175 participants worked as cybersecurity professionals and IT experts and government officials and academic researchers. Descriptive statistics to analyze data through frequency and percentage and mean and standard deviation and ranking analysis and Pearson correlation which studied the connection between AI adoption and cybersecurity performance indicators.* ***Results:*** *The study found that 81.1% of participants selected phishing attacks as their primary security risk while ransomware attacks received 77.7% and data breaches obtained 73.7% of the votes. Correlation data revealed that countries which adopt AI technology tend to experience better national security results with r = 0.77 and improved threat detection with r = 0.74 and stronger data protection with r = 0.69. The system provides multiple benefits to users but users encounter three major obstacles which include privacy concerns at 74.3% and insufficient qualified staff at 71.4% and costly setup expenses at 69.1%.* ***Novelty:*** *AI functions as a fundamental element which enhances both cybersecurity systems and protects national security interests.*

INTRODUCTION

Digital technologies have spread at an astonishing pace has reshaped modern societies operate by changing their communication networks and their defense systems and their economic systems and their governance structures [1]. The management of sensitive information together with vital operational functions now depends on digital systems which governments and organizations use through their interconnected networks [2]. Digital systems which people depend on have created new opportunities for cyber criminals to attack through data breaches and ransomware attacks and phishing campaigns and advanced persistent threats [3]. Critical infrastructures which include banking systems and healthcare services and energy grids and transportation networks and government databases depend mostly on digital platforms for their operation [4]. The systems will experience a chain reaction of problems when any disruption occurs which will produce financial losses and service stoppages and endanger the security of the nation [5]. Cybercriminals maintain their position at the top of hacking techniques by

combining automated systems with encryption decryption tools and social manipulation approaches to target security system weaknesses [6].

The current environment shows Artificial Intelligence (AI) as a solution which brings major changes to cybersecurity systems through its transformative power. The combination of machine learning with deep learning and behavioral analytics systems enables real-time detection of security anomalies and identification of malicious activities and immediate response to cyber threats [7]. AI-based systems operate differently from traditional methods because they learn from incoming data which enables their adaptation to new attack patterns [8]. AI systems become powerful threat detectors because they learn to identify new security threats which standard detection systems fail to identify. The cybersecurity field uses AI for multiple purposes which include intrusion detection systems and malware classification and phishing detection and network traffic analysis and real-time threat monitoring [9]. Security system receives advanced protection through predictive analytics which allows organizations to find system weaknesses before attackers can use them. Research data shows that AI-based systems increase threat detection accuracy between 85% and 90% while they speed up emergency responses in vital operational areas [10].

Moreover, AI serves as a crucial defense mechanism which protects essential infrastructure networks from potential threats. The banking industry and financial systems depend on AI technology to identify fraudulent transactions together with attempts to access accounts without authorization [11]. Healthcare systems require data protection systems to protect their confidential patient information. Artificial intelligence systems in energy and transportation sectors enable better system monitoring which prevents major system breakdowns from occurring [12]. AI-based cybersecurity solutions protect about 70% of major organizations which demonstrates how this technology has become essential for digital security protection. Cybercriminals have started using AI technology which creates a new problem that society needs to address [13]. The cyber arms race between defenders and attackers continues because AI technology enables attackers to create smart malware and automated phishing tools and flexible intrusion detection systems. The study aim Artificial Intelligence systems protect cybersecurity infrastructure while improving national security system performance. The research findings reveal Artificial Intelligence systems will defend national cybersecurity systems through permanent digital security and resilience protection. Digital technologies have spread at an astonishing pace has reshaped modern societies operate by changing their communication networks and their defense systems and their economic systems and their governance structures [1]. The management of sensitive information together with vital operational functions now depends on digital systems which governments and organizations use through their interconnected networks [2]. Digital systems which people depend on have created new opportunities for cyber criminals to attack through data breaches and ransomware attacks and phishing campaigns and advanced persistent threats [3]. Critical infrastructures which include

banking systems and healthcare services and energy grids and transportation networks and government databases depend mostly on digital platforms for their operation [4]. The systems will experience a chain reaction of problems when any disruption occurs which will produce financial losses and service stoppages and endanger the security of the nation [5]. Cybercriminals maintain their position at the top of hacking techniques by combining automated systems with encryption decryption tools and social manipulation approaches to target security system weaknesses [6].

The current environment shows Artificial Intelligence (AI) as a solution which brings major changes to cybersecurity systems through its transformative power. The combination of machine learning with deep learning and behavioral analytics systems enables real-time detection of security anomalies and identification of malicious activities and immediate response to cyber threats [7]. AI-based systems operate differently from traditional methods because they learn from incoming data which enables their adaptation to new attack patterns [8]. AI systems become powerful threat detectors because they learn to identify new security threats which standard detection systems fail to identify. The cybersecurity field uses AI for multiple purposes which include intrusion detection systems and malware classification and phishing detection and network traffic analysis and real-time threat monitoring [9]. Security system receives advanced protection through predictive analytics which allows organizations to find system weaknesses before attackers can use them. Research data shows that AI-based systems increase threat detection accuracy between 85% and 90% while they speed up emergency responses in vital operational areas [10].

Moreover, AI serves as a crucial defense mechanism which protects essential infrastructure networks from potential threats. The banking industry and financial systems depend on AI technology to identify fraudulent transactions together with attempts to access accounts without authorization [11]. Healthcare systems require data protection systems to protect their confidential patient information. Artificial intelligence systems in energy and transportation sectors enable better system monitoring which prevents major system breakdowns from occurring [12]. AI-based cybersecurity solutions protect about 70% of major organizations which demonstrates how this technology has become essential for digital security protection. Cybercriminals have started using AI technology which creates a new problem that society needs to address [13]. The cyber arms race between defenders and attackers continues because AI technology enables attackers to create smart malware and automated phishing tools and flexible intrusion detection systems. The study aim Artificial Intelligence systems protect cybersecurity infrastructure while improving national security system performance. The research findings reveal Artificial Intelligence systems will defend national cybersecurity systems through permanent digital security and resilience protection.

RESEARCH METHOD

Research Design

The research used a quantitative approach to study Artificial Intelligence (AI) systems affect the defense systems which protect national security and cybersecurity infrastructure. The design enables the exact measurement of AI implementation effects on cybersecurity performance through its evaluation of threat detection capabilities and data protection measures and infrastructure stability [14]. We collected numerical data from 175 respondents through a structured survey method which they used for their research. This study used quantitative methods to obtain objective results which produce statistics that remain reliable throughout every research phase. Correlation analysis to study variable connections which revealed AI adoption affects cybersecurity performance through its direction and strength [15]. The framework enables researchers to conduct field studies about AI-based cybersecurity security enhancements through its design which produces results that match different defense system variables [16].

Study Population and Sampling

The research population included cybersecurity professionals who specialized in this field together with IT specialists and officials from government agencies and scholars who studied this topic. we selected 175 respondents through purposive sampling because they wanted to include only people who understood the study topic and had relevant knowledge to share. The research benefits from this sampling approach because it allows experts to select samples through their knowledge instead of using general population preferences. Statistical analysis requirements through its 175-participant sample size which supports both percentage distribution and mean comparison and correlation analysis. The research method which targets specific samples produces better results because it collects data from experts who understand AI applications in cybersecurity systems and national security protection systems.

Data Collection Procedure

The research population included cybersecurity professionals specialized in this field together with IT specialists and officials from government agencies and scholars studied this topic. Purposive sampling because they wanted to include only people understood the study topic and had relevant knowledge to share [17]. The research benefits from this sampling approach because it allows experts to select samples through their knowledge instead of using general population preferences. Statistical analysis requirements through its 175-participant sample size which supports both percentage distribution and mean comparison and correlation analysis. Cybersecurity operations and research activities and policy-making activities [18], [19]. The research method which targets specific samples produces better results because it collects data from experts understand AI applications in cybersecurity systems and national security protection systems.

Data Analysis Techniques

Descriptive statistical methods together with inferential statistical techniques to analyze the data they had collected [20]. The study used descriptive statistics which included frequency and percentage and mean and standard deviation to present the results from respondent opinions. Pearson correlation analysis to determine how AI adoption relates to cybersecurity performance through the following equation (Rashid et al., 2023).

$$r = \frac{\sum(x - \bar{x})(y - \bar{y})}{\sqrt{\sum(x - \bar{x})^2 \sum(y - \bar{y})^2}}$$

The equation enables researchers to determine both the power of relationships between AI implementation and cybersecurity components and the direction which these relationships take. The ranking analysis process helped to identify which threats and benefits held the highest level of importance. Statistical analysis enables researchers to obtain accurate results which remain consistent and simple to understand [21].

RESULTS AND DISCUSSION

Results

Demographic Profile of Respondents

Demographic profile of respondents presents a well-balanced representation of professionals involved in cybersecurity and related fields as shown in **Table 1.** The study included 175 participants identified as 112 males and 63 females which created a study sample that showed balanced gender distribution. The survey results showed that most participants belonged to the 31–40 age range because this group represented 40.6% of respondents (71 people) while the 20–30 age group followed with 33.1% (58 people) and the 41–50 age group included 18.9% (33 people) and the 50+ age range consisted of 7.4% (13 people) which indicates that most participants worked during their middle career stage after gaining enough professional knowledge. The study included 49 cybersecurity experts who made up 28.0% of participants and 52 IT professionals who represented 29.7% of the group and 31 government officials who formed 17.7% of participants and 43 academic researchers who represented 24.6% of the sample. We obtained data from various essential cybersecurity stakeholders which created trustworthy and in-depth information for their AI-based infrastructure analysis.

AI Effectiveness in Cybersecurity Infrastructure

The results from **Figure 1** indicate a strong positive perception of Artificial Intelligence (AI) in enhancing cybersecurity infrastructure across multiple functional domains. Among the evaluated AI functions, real-time monitoring achieved the highest effectiveness level, with 63.4% of respondents rating it as highly effective, followed by phishing detection at 61.7% and threat detection at 58.3%. Malware identification and intrusion prevention also showed strong performance, with combined "highly effective" and "effective" responses exceeding 80% in all categories. Only a small proportion of

respondents considered AI functions ineffective, ranging from 3.4% to 5.1%, indicating minimal dissatisfaction.

Cybersecurity Threats Affecting National Infrastructure

The data from **Table 2** shows the primary cybersecurity dangers which national infrastructure systems face according to answers from 175 study participants. Phishing attacks became the top security risk because 81.1% of respondents selected this option which shows how social engineering methods have become common practice. Ransomware attacks surpassing 77.7% demonstrate how this threat has expanded its influence by blocking data access while criminals demand money from victims. Data breaches stand as the third most common security breach because 73.7% of organizations experience unauthorized access to their sensitive government and organizational information. The widespread occurrence of malware attacks which reached 69.1% shows that computer systems continue to face threats from harmful software. The 56.0% insider threat statistic reveals that organizations face dangers from people who work inside their systems while keeping their authorized access. Distributed Denial of Service attacks received the lowest rating of 52.0% but they continue to pose a major threat because they cause service interruptions.

Benefits of AI Integration in National Cybersecurity Systems

In **Table 3** provides a summary of how people view the advantages which national cybersecurity systems obtain through their AI system deployment. The research shows that AI detection systems identify cyber threats at their fastest speed because threat detection reached the top spot with an average score of 4.61 (SD = 0.48). Security of sensitive information receives strong support from AI systems which users agree upon according to their 4.52 average rating (SD = 0.57). The third position (M = 4.45, SD = 0.63) shows that automated incident response systems deliver improved cyber incident management efficiency. AI systems reduce human mistakes during cybersecurity operations because they decrease the need for human involvement which scores 4.37 (SD = 0.71). The fifth position (M = 4.31, SD = 0.69) shows that infrastructure resilience improvement leads to better system defense against attacks. The research data shows that cost efficiency obtained the lowest score (M = 4.14, SD = 0.78) however participants still viewed it positively.

Challenges of AI-Based Cybersecurity Implementation

The main obstacles which people identified for AI cybersecurity system implementation appear in **Figure 2.** The data shows that privacy issues represent the most critical problem because 74.3% of respondents agree which proves people strongly fear their personal data will be misused and monitored. The second highest challenge at 71.4% shows that organizations face problems because they do not have enough specialists who can handle their complex AI security solutions. The financial cost of implementation stands as a major challenge which 69.1% of respondents identified because funding remains a key obstacle for deploying extensive systems. Security decision-making shows a lack of human interaction because 62.9% of people agree

automation has taken over their systems. The AI system faces lower bias levels which reach 57.7% but these numbers still show that algorithms will make wrong decisions.

Correlation Analysis Between AI Adoption and Cybersecurity Performance

Correlation analysis between AI adoption and cybersecurity performance indicators appears in **Figure 3.** The results demonstrate strong positive relationships which exist between all the variables. The highest national security enhancement correlation with AI adoption reached r = 0.77 which means AI adoption leads to strong national cyber defense systems. The data shows a strong connection between threat detection and r = 0.74 which proves the system improved its ability to detect cyber threats quickly. The relationship between data protection and AI adoption reaches r = 0.69 which indicates that AI adoption leads to better protection of sensitive data. The system shows moderate resistance to cyber threats because its infrastructure resilience reaches an r value of 0.66. The cybersecurity variables display strong connections between their components because threat detection connects with data protection at r = 0.72 and infrastructure resilience at r = 0.71.

Discussion

Artificial Intelligence (AI) functions as a vital security system which protects national security infrastructure and strengthens cybersecurity defense systems [22]. AI-based systems generate better threat detection results while protecting data and enhancing system protection throughout essential digital infrastructure systems [23]. The survey participants completely agreed that AI technology brings better real-time monitoring capabilities which result in faster cyber incident responses that protect modern cybersecurity systems ([24]. National infrastructure suffers most from three major cybersecurity threats which include phishing attacks at 81.1% and ransomware at 77.7% and data breaches at 73.7%. The current situation matches worldwide cybersecurity patterns because social engineering attacks and ransomware attacks have shown fast growth in numbers. The threat evaluation indicates that current security measures cannot protect against these dangers because they need smart automated systems to detect and stop threats during their early stages [25].

Cybersecurity threat detection and response systems operate effectively because of machine learning and deep learning algorithms which function as AI technologies [26]. AI technology enhances phishing detection systems and malware classification and intrusion prevention systems while receiving positive feedback from more than 80% of respondents across all categories. AI systems perform better than standard approaches when they analyze big data sets while they identify strange patterns and discover new security risks [27]. The system needs this feature to safeguard its complicated network of digital systems which link together. The research proved that AI adoption created a direct effect on cybersecurity results through its correlation analysis. AI adoption generated the highest connection strength with national security enhancement through a correlation coefficient of 0.77. AI adoption produced a strong correlation with threat detection systems which reached 0.74 and data protection systems which reached 0.69.

Organizations which adopt AI technology will achieve better cybersecurity outcomes. The research results match earlier studies which prove that AI technology serves as the main factor which drives security systems to adopt digital transformation practices [28].

Respondents identified two main benefits from AI integration because they could detect threats more quickly at M = 4.61 and protect their data better at M = 4.52. The study proves that AI systems boost operational performance while they establish better security systems which produce precise and dependable results. The automated incident response systems perform two essential functions because they decrease human work requirements and they shorten attack response times which results in quicker system recovery and reduced system damage [29]. The system provides multiple benefits yet users encountered various operational difficulties when they started using it. The main problem according to 74.3% of respondents involves privacy issues because AI systems generate worries about monitoring activities and improper use of personal information. The shortage of trained staff members at 71.4% creates a major obstacle because AI systems need people with high levels of technical knowledge to function properly. The high costs of implementation at 69.1% create a barrier which stops developing nations and smaller businesses from using AI technology. Organizations need to solve their dependency on automated systems because these systems restrict human monitoring of vital decision-making procedures [30].

CONCLUSION

Fundamental Finding: Artificial Intelligence (AI) operates as a critical force which strengthens cybersecurity systems and boosts national defense capabilities. The research shows that AI technology provides better threat detection systems which protect data through continuous security monitoring of operational systems. The research shows that AI implementation creates a strong connection which improves cybersecurity performance. **Implication:** The most important security threats today include phishing attacks and ransomware infections together with data breaches which require sophisticated AI defense systems. **Limitation:** The system needs to solve three major problems which include privacy issues and insufficient trained staff and expensive system deployment requirements. **Future Research:** Future research should further examine how AI defense systems can address privacy issues, improve staff training, and reduce expensive system deployment requirements.

REFERENCES

[1] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, no. 3, 2021, doi: 10.1007/s42979-021-00557-0.

[2] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability*, vol. 13, no. 6, p. 3196, 2021, doi: 10.3390/su13063196.

[3] Y. Jun, A. Craig, W. Shafik, and L. Sharif, "Artificial intelligence application in cybersecurity and cyberdefense," *Wirel. Commun. Mob. Comput.*, vol. 2021, p. 1, 2021, doi: 10.1155/2021/3329581.

[4] O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, and F. Di Giandomenico, "Security-Informed safety analysis of autonomous transport systems considering AI-Powered Cyberattacks and protection," *Entropy*, vol. 25, no. 8, p. 1123, 2023, doi: 10.3390/e25081123.

[5] A. Alzahrani and T. H. H. Aldhyani, "Design of efficient based artificial intelligence approaches for sustainable of cyber security in smart industrial control system," *Sustainability*, vol. 15, no. 10, p. 8076, 2023, doi: 10.3390/su15108076.

[6] M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas, and Z. H. Abbas, "The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges," *Artif. Intell. Rev.*, vol. 55, no. 7, pp. 5215–5261, 2022, doi: 10.1007/s10462-022-10143-2.

[7] A. Carlo *et al.*, "The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications," *Journal of Space Safety Engineering*, vol. 10, no. 4, pp. 474–482, 2023, doi: 10.1016/j.jsse.2023.08.002.

[8] J. Andraško, M. Mesarčík, and O. Hamuľák, "The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework," *AI Soc.*, vol. 36, no. 2, pp. 623–636, 2021, doi: 10.1007/s00146-020-01125-5.

[9] Z. Lv, D. Chen, R. Lou, and A. Alazab, "Artificial intelligence for securing industrial-based cyber–physical systems," *Future Generation Computer Systems*, vol. 117, pp. 291–298, 2020, doi: 10.1016/j.future.2020.12.001.

[10] S. S. Morse *et al.*, "Prediction and prevention of the next pandemic zoonosis," *The Lancet*, vol. 380, no. 9857, pp. 1956–1965, 2012, doi: 10.1016/S0140-6736(12)61684-5.

[11] G. L. Sanclemente, "Reliability: understanding cognitive human bias in artificial intelligence for national security and intelligence analysis," *Security Journal*, vol. 35, no. 4, pp. 1328–1348, 2021, doi: 10.1057/s41284-021-00321-2.

[12] D. S. Reveron and J. E. Savage, "Cybersecurity convergence: digital human and national security," *Orbis*, vol. 64, no. 4, pp. 555–570, 2020, doi: 10.1016/j.orbis.2020.08.005.

[13] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for businesses Resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, p. 6666, 2023, doi: 10.3390/s23156666.

[14] A. Bouramdane, "Cyberattacks in Smart Grids: Challenges and solving the Multi-Criteria Decision-Making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process," *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 662–705, 2023, doi: 10.3390/jcp3040031.

[15] T. Saheb and T. Saheb, "Topical review of artificial intelligence national policies: A mixed method analysis," *Technol. Soc.*, vol. 74, p. 102316, 2023, doi: 10.1016/j.techsoc.2023.102316.

[16] I. H. Sarker, "Multi-aspects AI -based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview," *Security and Privacy*, vol. 6, no. 5, pp. 1–21, 2023, doi: 10.1002/spy2.295.

[17] J. Burton, "Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence," *Technol. Soc.*, vol. 75, p. 102262, 2023, doi: 10.1016/j.techsoc.2023.102262.

[18] A. Pinto, L. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on Intrusion Detection Systems based on Machine learning Techniques for the protection of Critical Infrastructure," *Sensors*, vol. 23, no. 5, p. 2415, 2023, doi: 10.3390/s23052415.

[19] L. Pinto, M. R. Tapia-Rodríguez, F. Baruzzi, and J. F. Ayala-Zavala, "Plant antimicrobials for food quality and safety: Recent views and future challenges," *Foods*, vol. 12, no. 12, p. 2315, 2023, doi: 10.3390/foods12122315.

[20] F. Muheidat and L. Tawalbeh, "Artificial intelligence and blockchain for cybersecurity applications," in *Studies in big data*, 2021, pp. 3–29. doi: 10.1007/978-3-030-74575-2_1.

[21] A. Kumar and P. Yadav, "Experimental investigation on alkaline treated natural fiber reinforced composites," *J. Eng. Mech.*, vol. 2, no. 4, pp. 25–31, 2024.

[22] T. Mazhar *et al.*, "Analysis of IoT security challenges and its solutions using artificial intelligence," *Brain Sci.*, vol. 13, no. 4, p. 683, 2023, doi: 10.3390/brainsci13040683.

[23] M. Mylrea *et al.*, "BioSecure Digital Twin: manufacturing innovation and cybersecurity resilience," in *Lecture notes in computer science*, 2021, pp. 53–72. doi: 10.1007/978-3-030-89385-9_4.

[24] S. Gerke, T. Minssen, and G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," in *Elsevier eBooks*, 2020, pp. 295–336. doi: 10.1016/b978-0-12-818438-7.00012-5.

[25] M. Warner, "Cybersecurity: a Pre-history," *Intelligence & National Security*, vol. 27, no. 5, pp. 781–799, 2012, doi: 10.1080/02684527.2012.708530.

[26] S. Fatima, K. C. Desouza, and G. S. Dawson, "National strategic artificial intelligence plans: A multi-dimensional analysis," *Econ. Anal. Policy*, vol. 67, pp. 178–194, 2020, doi: 10.1016/j.eap.2020.07.008.

[27] S. Sadik, M. Ahmed, L. F. Sikos, and A. K. M. N. Islam, "Toward a sustainable cybersecurity ecosystem," *Computers*, vol. 9, no. 3, p. 74, 2020, doi: 10.3390/computers9030074.

[28] P. Sharikov, "Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination," *Bulletin of the Atomic Scientists*, vol. 74, no. 6, pp. 368–373, 2018, doi: 10.1080/00963402.2018.1533185.

[29] T. C. Truong, I. Zelinka, J. Plucar, M. Čandík, and V. Šulc, "Artificial intelligence and cybersecurity: past, presence, and future," in *Advances in intelligent systems and computing*, 2020, pp. 351–363. doi: 10.1007/978-981-15-0199-9_30.

[30] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Comput. Appl.*, vol. 34, no. 18, pp. 15241–15271, 2022, doi: 10.1007/s00521-022-06959-2.

***Chowdhury Amin Abdullah (Corresponding Author)**
Seidenberg School of Computer Science and Information Systems, Pace University, New York, United States
E-mail: chowdhury.aminabdullah@pace.edu

Md Jahidul Islam Ridoy
Independent Researcher, New York, United States