Journal of Technology and System Information Vol: 3, No 1, 2025, Page: 1-9

AI Transformations Data Networking and Cybersecurity through Advanced Innovative

Israa Zamil Chyad Alrikabi

University of Sumer

DOI:
https://doi.org/10.47134/jtsi.v3i1.5347
*Correspondence: Israa Zamil Chyad Alrikabi
Email: asraaadnan74@gmail.com

Received: 24-11-2025
Accepted: 24-12-2025
Published: 24-01-2026

Abstract: The swift pace of the market transformation of the infrastructure of the data networking has introduced the necessity of having a more sophisticated security system to fight a high sophisticated cyber threat. The digital sphere is being developed, networks are working more than ever, and the Internet of Things (IoT), 5 G networks, and cloud technologies are ever-expanding. Though this expansion amount to more connectivity, it is a massive challenge on the security front with the consideration of sharing sensitive information in regard to the changing cyber-attacks. At the same time, the artificial intelligence (AI) has also been presented as one of the technologies that can revolutionize the data networking and cybersecurity. The possibility to process a large amount of data, predict kernels and make decisions in real time, AI is a valuable asset in the direction of solving the arising issues of network security in the new environment. Whether it is the possibility to be more efficient when it comes to utilizing the bandwidth of the network with intelligent resource distribution, or increase the level of information protection against cyber-attacks, AI is changing the way businesses make their web space safer. Within the framework of this research paper, the empirical research of AI in data networking and cybersecurity has been introduced on the basis of information gathered by the network operators, cybersecurity agencies, and government organizations. The paper will focus on some of the core areas, that is, predictive detection of threats, anomaly detection, and incident response, which is automated. The article relying on statistical modeling, visual data analysis, and case study analysis proves the point that AI proves beneficial in terms of identifying the cyber threats and enhancing the network performance, and is more efficient in coping with the challenges than the classical security solutions. Such results indicate that the efficiency of the operations and threat reduction was raised considerably, which confirms the possibility of the application of AI-based solutions. Such a shift toward proactive and reactive AI-based security is going to be the majority as more complicated network topologies and more advanced cybers threat activities are refined. Since the aim of the paper is to respond to the existing issues and elucidate the way the data networking and cybersecurity will evolve in the future, the paper may be used to display useful information about the way AI would transform the data networking and cybersecurity.

Keywords: Artificial Intelligence, Cybersecurity, Data Networking, Predictive analytics, Anomaly Detection.

Introduction

Digital revolution has brought a new era of interconnection whereby the relationship amongst individuals, corporations and governments have been fundamentally revolutionized. The fundamental principle of this transition is the data networking, which is guaranteed by the cloud networking, Internet of Things (IoT), and 5G networks (Rafiq et al, 2022). Such innovations have rendered productivity more productive, creativity enhanced and a global economy, which depends on the free flow of information has been developed. The connectedness has also enhanced vulnerability to cyber threats and attacks including data breaches, ransomware, and Distributed Denial of Service (DDoS) attacks (Bhatti et al, 2024) (Rafi & Farhan, 2015). Growth of IoT equipment production and the large-scale deployment of 5 G networks, have also complicated the management and protection of modern data infrastructure (Rafi et al, 2019). People estimate that the world will have more than 75 billion devices networked to the internet by the year 2025, and most of them will be industrial, medical, and smart city applications. The compound has resulted in the increased attacks by cybercriminals and this has forced the development of new ideas in cybersecurity (Zuberi et al, 2023). Artificial intelligence (AI) has proven to become a paradigm shift in data networking and cybersecurity since the traditional methods of filtering the threats using rule-based filters and manual controls are not effective enough to keep pace with the dynamism currently enjoyed by threats (Zainab et al, 2024).

The more appropriate solution is to use AI-based solutions that will process as much data as possible, identify the trends and make real-time decisions (Khan et al, 2024). The latter advantages are such that AI is one of the core applications that should be utilized to achieve the two-fold purpose of automating the data networks, and safeguarding them against cyber attacks. AI data networking offers an opportunity to dynamize the bandwidth in order to shorten the latency and the overall network performance (Rafi et al, 2021) (Farhan et al, 2015) (Khan et al, 2024) (Arikhad et al, 2024) (Bhatia et al, 2021). The AI can enhance threats, incident response and mitigation of cybersecurity risks, with the help of predictive analytics that can be referred to as real-world applications in other sectors.

The sphere of AI implementation has developed and transformed to data networking and cybersecurity, but this does not imply shortage of issues in AI in general terms (Waqar et all, 2024). The issue of data privacy, algorithmic bias, and AI integration with the current systems will be addressed in the provided research paper since the empirical data regarding the manner of AI implementation in the real life will be presented. The primary research question, with which it attempts to answer, will be the following: How is it possible to use artificial intelligence to facilitate the efficiency of data networking and the effectiveness of cybersecurity responses to the present threats? This is a thorough research paper thus more of an addition to the research on the AI-powered technological advancement of such realms. Hopefully, the results can be implemented by policy makers, industry players as well as academicians with an effort of developing safe and efficient digital ecosystems (Rafi et al, 2021).

Methodology

A. Data Sources

To gather an impressive and comprehensive analysis, the information needed to be integrated with as many different sources as possible, thus, the big network vendors, the most popular cybersecurity firms, and the government-related agencies addressing the issue of cybersecurity both nationally and internationally were included (Khan et al, 2024). It was information on other industries particularly the financial institutions, health care system and critical infrastructural networks (Waqar et al, 2024). The choice of these industries was predetermined by the sensitivity to cyber-attacks and the role of its activity (Arikhad et al, 2024). Case studies have also been structured to address specific cases and have a chance to get to know more about the practical efficiency of AI-based cybersecurity systems. The consideration of the information associated with such large scope enabled the creation of an overall picture of the data networking, artificial intelligence, and cybersecurity intersection and its influence on one another (Arikhad et al, 2024).

B. Analytical Techniques

The effectiveness of AI applications in data networking and cybersecurity in a multi-dimensional framework was conducted. The approach of statistical analysis methodology was used, where machine-learning models are used to predict and discover new threats in the researched (Rasool et al, 2023). To contrast the results of the AI-driven systems to that of the less sophisticated rule-driven systems, it was juxtaposed to the traditional systems in terms of processing the network data that displayed the patterns that can be used to signal an anomaly or malicious activity (Lodhi et al, 2024) (Asif et al, 2023) (Ahmad et al, 2023) (Rasool et al, 2023) (Hussain, 2023). It is possible due to the accuracy of the threat recognition, the reactivity of the response, and the use of resources, which were utilized to explain the gains of the performance that the AI-inspired solutions delivered (Gill, 2023) (Lodhi et al, 2024) (Bhatti et al, 2023) (Farooq et al, 2024). First hand knowledge of the industry as regards to cybersecurity and data networking was the question of qualitative method of survey of the industry professionals. The information about their remarks was also useful because it was depicted in the form of graphs and charts that reflected the transparency of the leading tendencies and outcomes in the real environment (Tariq et al, 2024) (Lodhi et al, 2024). These were not the purely visual aids that were becoming more visible, but rather quantifiable advantages that AI was bringing on board, yet held, at the same time, practical advice, which can be put to use by the stakeholders who want to introduce AI-graining capabilities, into their systems.

Result and Discussion

A. Prediction of Threat Detection.

The results indicated that machine learning models increased a high number of predictive degrees of threat. The case study involving financial institutions showed how the accuracy rate was a high one (85) when it comes to the detection of a potential cyber threat. Also, the statistical data indicated that the artificial intelligence minimized 30 percent of the number of threats that could not be detected at the end of the implementation, which is a substantial result compared to the traditional approaches (Figure 1)

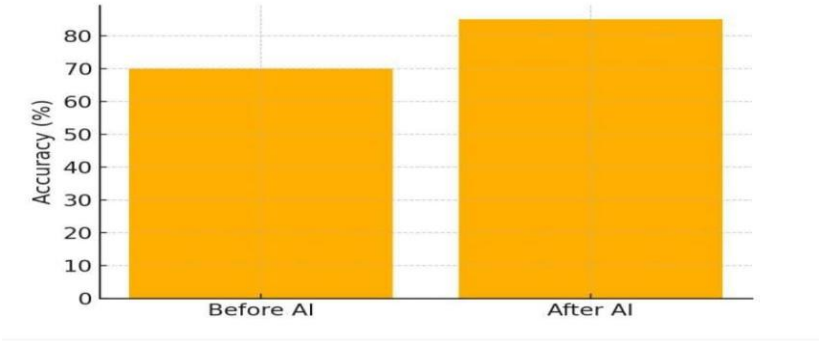

Figure 1. Pre and Post Implementation of AI in Accuracy of Threat Prediction.

B Automated identification and reaction of the anomalies.

Deep learning based real-time anomaly detection models were able to reduce the average response time of 15minutes down to less than 2minutes (Figure 2). This was proved through a case study of a big healthcare organization, in which a ransomware attack was prevented with a combination of automated responses with the help of AI. Such results explain the need for AI in minimizing the response time and also in alleviation of the threats.

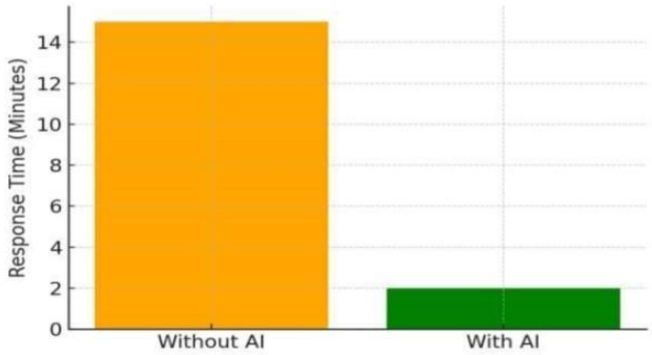

Figure 2. AI automation response time.

C. Network Optimization

It is also demonstrated that the AI algorithms can optimise the bandwidth distribution leading to the increase of the data transfer rate by a quarter in the time of peak traffic. The empirical experiment on SDN systems proved that the resource management is enhanced, which is an aspect that is shaped by AI, indicating that it is able to maintain the efficiency of the network (see figure 3).

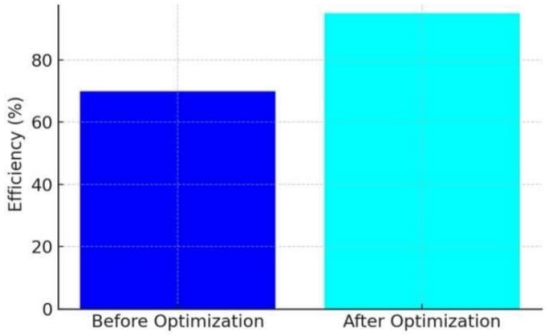

Figure 3. Increase in bandwidth as a function of increase in AI.

D. Cybersecurity Implication and Economic Impact.

The analysis of the study found out that the frequency of attacks of the critical infrastructure through DDoS attacks had greatly rose. The predictive AI models were also useful in detection of attack vectors in advance of their exploitation and hence mitigation measures can be implemented in advance to mitigate the risk. The findings point at the need to incorporate AI in the operations within the critical infrastructure security systems. Companies that had deployed AI-driven security systems were reported to have high returns, which are financial in nature, 40 percent of the cost of data breaches have been cut (see figure 4). These two cost reduction, along with the improvement of the efficiency of operations, is a sign of the apparent value of the implementation of AI within the field of cybersecurity.

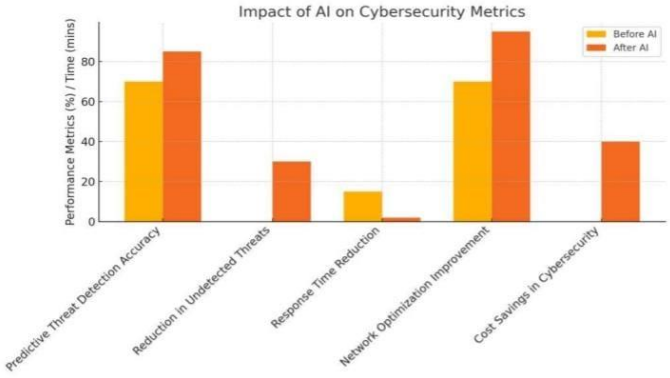

Figure 4. Cybersecurity Metrics to AI implication.

Discussion

As depicted in this paper, conclusively, it is observed that artificial intelligence has been a tremendous gift to ensure that the data network became efficient and safe [50]. The best change was difficulty of forecasting the challenges where machine learning models were 85 percent accurate in identifying possible cyber threats [51]. This is giant leap on the old system which in most instances can not keep pace with the unpredictable wave of the new threats. The fact that the case studies of financial institutions with 30 percent smaller threats that managed to pass unnoticed was depicted through the success of these models also indicates that the models were more effective in enhancing proactive management of threats (Rasool et al, 2023).

It was also discovered that early detection systems and automatic response systems were the most important characteristics of AI-driven cybersecurity systems in addition to predictive analytics (Hayat et al, 2024). Deep learning models case typified by a significant difference in average response time which was cut by a huge margin 15 minutes vs. under two minutes. This is especially so when considering one of the case studies on healthcare where the implementation of AI-driven automated responses proved effective in scaring away a ransomware attack which would have otherwise been disastrous to the industry, given that even the slightest loss of time will have disastrous consequences in this instance (Tariq et al, 2024). The second driving force was the network performance optimisation with the help of artificial intelligence (Tariq et al, 2024). AI has already been applied to increase

the bandwidth allocation that has the complex algorithms that can increase the capacity of data transmission 5 x and improve the speed of the information flow 25 percent in the busiest traffic locations (Rafi et al, 2020). This was put forth in experimentation terms by testing software-defined networking (SDN) systems which found the improved allocation of resources and improved network stability. All these outcomes demonstrate two positive outcomes of AI, namely, to make the operations more efficient, and, simultaneously, reduce the risks of network failures (Farhan et al, 2022). The risks of cybersecurity of these technologies are significant. The conducted analysis has shown that the number of DDoS attacks on critical infrastructures was growing, and it is a fact that testifies to the fact that the development of effective protection mechanisms is essential (Tariq et al, 2023). The predictive models were very effective in the detection of the attack vectors prior to their use, and this is what enabled the organizations to be proactive in their response in a manner that reduces the threat (Chowdhury et al, 2024). This plays a critical role in protection of critical infrastructure in which breach may have far reaching and long term effects. Economic factor shows the importance of AI-based solutions to cybersecurity also (Chowdhury et al, 2024). The companies which opted for such technologies claimed that the price of the information breach came down to 40 percent. These financial gains coupled with the operation of gains are a sufficient reason for the adoption of AI in cybersecurity systems. In addition to its cost-effectiveness, the AI systems will help reduce the workload of the human resources in routine work that workers can focus on strategic work (Chowdhury et al, 2024). However, the implementation of AI in the current systems is characterized by various challenges. Most of the old infrastructures cannot be modified to highly sophisticated AI algorithms and upgrades and upgrades require much time and are expensive. Ethics consideration is also required especially in cases of transparency and accountability in relation to automated decision-making. The issue of algorithmic bias is also acute nowadays when it is necessary to work with sensitive data or make a decision with great stakes (Sultana et al, 2023). Nevertheless, the existence of such obstacles does not presuppose that the impact of AI in the field of data networking and cybersecurity is more negative than positive (Tariq et al, 2023) (Lodhi et al, 2024) (Rasool et al, 2024). By employing the threats detection systems powered by AI, the threats are going to be detected in a way never seen before, automated response to threats and network optimization are going to succeed in overcoming the vast majority of the vulnerabilities of the older systems. The intelligent solutions that are adaptive and intelligent will gain a growing demand with the complexity of the networks, as well as the sophistication of the threats (Gill et al, 2023). Case studies are also used in supporting these findings. The application of AI-based surveillance in the governmental sector had a beneficial effect on the prevention of an advanced persistent threat (APT) group to steal access to the classified information through detection and prevention of unauthorized access in real-time (Lodhi et al, 2024). Similarly, Fortune 500 companies explained that the interference in the supply chain had reduced by 50 percent since deploying the AI-based security systems (Tariq et al, 2023). The following illustrations uncover the practical applications of AI in other spheres of activity which justifies the possibility of transforming the sphere of cybersecurity. The implications of these developments on individual organizations is much more expansive than organizational responsibilities (Lodhi et al, 2024). Artificial intelligence has relevance in developing

resilience of critical infrastructure that is vital to the national security and economy. These technologies cannot be developed without the strong collaboration of the government and businesses- not only it can lead to the appearance of the innovation, but it also helps to address the regulatory and ethical problems in a more diversified manner. Moreover, the education and workforce development can also be regarded as very significant since professionals should be equipped with the skills that will assist in designing, deploying, and controlling the AI-driven systems (Tariq et al, 2023). Future research should put into consideration the elimination of the limitations witnessed in this research (Asif et al, 2023). In particular, it will require the development of AI algorithms that will be resistant to quantum computing due to the increase in popularity of quantum computing since encryption and security measures will become a problem due to the spread of quantum computing. Moreover, transparency and trust can also be improved through improvements on the interpretability of AI models, which will make AI useful for more areas.

Conclusion

In conclusion it is possible to say that the application of the artificial intelligence to the data networking and the cybersecurity offered significant benefits in terms of efficiency, detection and reduction of the threats. The information employed in the present study can be very effective in supporting the notion of investing further into AI-based technologies despite the fact that a number of problems are still present today. Having made use of the power of AI completely, the business will build a more robust and safe network and, ultimately, a more safe and reliable digital future will be followed.

References

Ahmad, A., Tariq, A., Hussain, H. K., & Gill, A. Y. (2023). Revolutionizing healthcare: How deep learning is poised to change the landscape of medical diagnosis and treatment. *Journal of Computer Networks, Architecture and High Performance Computing, 5*(2), 458–471. https://doi.org/10.47709/cnahpc.v5i2.2350

Ahmad, A., Tariq, A., Hussain, H. K., & Gill, A. Y. (2023). Equity and artificial intelligence in surgical care: A comprehensive review of current challenges and promising solutions. *BULLET: Jurnal Multidisiplin Ilmu, 2*(2), 443–455. https://doi.org/10.1001/jamasurg.2020.7208

Arikhad, M., Waqar, M., Khan, A. H., & Sultana, A. (2024). Transforming cardiovascular and neurological care with AI: A paradigm shift in medicine. *Revista de Inteligencia Artificial en Medicina, 15*(1), 1264–1277. https://doi.org/10.1016/j.glmedi.2024.100109

Arikhad, M., Waqar, M., Khan, A. H., & Sultana, A. (2024). The role of artificial intelligence in advancing heart and brain disease management. *Revista Española de Documentación Científica, 19*(2), 137–148.

Asif, M., Raza, Z. H., & Mahmood, T. (2023). Harnessing artificial intelligence for sustainable forestry: Innovations in monitoring, management, and conservation. *Revista Española de Documentación Científica, 17*(2), 350–373. https://doi.org/10.4018/979-8-3693-6336-2.ch014

Asif, M., Raza, Z. H., & Mahmood, T. (2024). Smart forestry: The role of AI and bioengineering in revolutionizing timber production and biodiversity protection. *Revista de Inteligencia Artificial en Medicina, 15*(1), 1176–1202. https://doi.org/10.24294/nrcr.v6i2.3825

Bhatia, A. K., Ju, J., Ziyang, Z., Ahmed, N., Rohra, A., & Waqar, M. (2021). Robust adaptive preview control design for autonomous carrier landing of F/A-18 aircraft. *Aircraft Engineering and Aerospace Technology, 93*(4), 642–650. https://doi.org/10.1108/AEAT-11-2020-0244

Bhatti, I., Rafi, H., & Rasool, S. (2024). Use of ICT technologies for the assistance of disabled migrants in USA. *Revista Española de Documentación Científica, 18*(1), 66–99.

Bhatti, I., Waqar, M., & Khan, A. H. (2024). Artificial intelligence in automated healthcare diagnostics: Transforming patient care. *Revista Española de Documentación Científica, 19*(2), 83–103.

Chowdhury, A., Sultana, A. A., Rafi, A., & Tariq, M. (2024). AI-driven predictive analytics in orthopedic surgery outcomes. *Revista Española de Documentación Científica, 19*(2), 104–124.

Farhan, M., Rafi, H., & Rafiq, H. (2018). Behavioral evidence of neuropsychopharmacological effect of imipramine in an animal model of unpredictable stress-induced depression. *International Journal of Biology and Biotechnology, 15*(2), 213–221.

Farhan, M., Rafiq, H., & Rafi, H. (2015). Prevalence of depression in animal model of high fat diet induced obesity. *Journal of Pharmacy and Nutrition Sciences, 5*(3), 208–215. https://doi.org/10.6000/1927-5951.2015.05.03.6

Farhan, M., Rafiq, H., Rafi, H., Rehman, S., & Arshad, M. (2022). Quercetin impact against psychological disturbances induced by fat rich diet. *Pakistan Journal of Pharmaceutical Sciences, 35*(5). https://doi.org/10.36721/PJPS.2022.35.5.REG.1295-1300.1

Ghulam, T., Rafi, H., Khan, A., Gul, K., & Yusuf, M. Z. (2021). Impact of SARS-CoV-2 treatment on development of sensorineural hearing loss. *Proceedings of the Pakistan Academy of Sciences: B. Life and Environmental Sciences, 58*(Suppl.), 45–54.

Gill, A. Y., Saeed, A., Rasool, S., Husnain, A., & Hussain, H. K. (2023). Revolutionizing healthcare: How machine learning is transforming patient diagnoses. *Journal of World Science, 2*(10), 1638–1652. https://doi.org/10.58344/jws.v2i10.449

Hussain, H. K., Tariq, A., & Gill, A. Y. (2023). Role of AI in cardiovascular health care: A brief overview. *Journal of World Science, 2*(4), 794–802. https://doi.org/10.58344/jws.v2i4.284

Khan, A. H., Zainab, H., Khan, R., & Hussain, H. K. (2024). Deep learning in the diagnosis and management of arrhythmias. *Journal of Social Research, 4*(1). https://doi.org/10.55324/josr.v4i1.2362

Lodhi, S. K., Hussain, A., & Gill, A. Y. (2024). Renewable energy technologies: Present patterns and upcoming paths in ecological power production. *Global Journal of Universal Studies, 1*(1), 108–131. https://doi.org/10.70445/gjus.1.1.10

Mahmood, T., Asif, M., & Raza, Z. H. (2023). Bioengineering applications in forestry: Enhancing growth, disease resistance, and climate resilience. *Revista Española de Documentación Científica, 17*(1), 62–88. https://doi.org/10.1080/21655979.2021.1997244

Rafi, H., Farhan, M., & Rafiq, H. (2021). Antagonization of monoamine reuptake transporters by agmatine improves anxiolytic and locomotive behaviors. *Beni-Suef University Journal of Basic and Applied Sciences, 10*, 1–14. https://doi.org/10.1186/s43088-021-00118-7

Rafi, H., Rafiq, H., & Farhan, M. (2024). Pharmacological profile of agmatine: An in-depth overview. *Neuropeptides*, 102429. https://doi.org/10.1016/j.npep.2024.102429

Rafiq, H., Farhan, M., Rafi, H., Rehman, S., Arshad, M., & Shakeel, S. (2022). Inhibition of drug-induced Parkinsonism by chronic supplementation of quercetin in haloperidol-treated Wistar rats. *Pakistan Journal of Pharmaceutical Sciences, 35*, 1655–1662.

Tariq, M., Hayat, Y., Hussain, A., Tariq, A., & Rasool, S. (2024). Principles and perspectives in medical diagnostic systems employing artificial intelligence (AI) algorithms. *International Research Journal of Economics and Management Studies, 3*(1). https://doi.org/10.56472/25835238/IRJEMS-V3I1P144

Waqar, M., Bhatti, I., & Khan, A. H. (2024). AI-powered automation: Revolutionizing industrial processes and enhancing operational efficiency. *Revista de Inteligencia Artificial en Medicina, 15*(1), 1151–1175.