International Journal of Advanced Engineering **ISSN: 2457-0397**

Vol. 6, Issue III, Jul-Sep, 2023 http://bharatpublication.com/current-issue.php?jID=29/IJAE

Employability of Artificial Intelligence Algorithms for Enhancing the Effectiveness of Data Access Security Against Cyber Threats[1]

Suchit Lamba

NIIT University, Neemrana, Rajasthan, India

ABSTRACT

Artificial intelligence (AI) research, focused on emulating intelligent behaviour in artificial systems, has long been influenced by human cognition. Repetitive learning is a crucial component of AI, with its implications on global security being of paramount concern. Future endeavours in social and natural sciences must acknowledge this significance. Given that numerous services are now delivered through online platforms, security measures and effective data governance are imperative outcomes. The integration of AI into society significantly impacts both industrial and digital revolutions. Safeguarding accessibility in the use of electronic devices is crucial across various applications, including data mining, analytics, bitcoin, and blockchain technology, to mitigate online risks associated with data access. The proliferation of internet-based applications increases the likelihood of cyber threats emerging from uncontrolled data access. To address these risks and optimize the benefits of widespread AI adoption, this study proposes high-security data access management utilizing AI, offering a solution for innovative global commerce ventures. The efficacy of this approach is evaluated across various metrics, including Accuracy, Recall, and Specificity, ensuring robust performance across different methods. Through comprehensive analysis, this study provides insights into the most effective strategies for managing cyber risks in AI-enabled environments.

INTRODUCTION

This paper explores the immense potential of integrating artificial intelligence (AI) into the security technology landscape. AI, including machine learning tools, has the capability to generalize information or leverage expertise to solve novel problems. This opens up a world of possibilities for enhancing security systems management. Examples of AI include expert systems, artificial neural networks (ANN), kernel machines, and fuzzy set theory. AI can significantly benefit various data mining activities, such as modelling, classification, regression, association analysis, cluster analysis, outlier analysis, and evolution analysis, particularly when data is available.

While neural networks have their practical limitations, such as their reliance on basic knowledge about the issue and the necessity for previous data to solve problems effectively, AI offers a pathway to address these challenges. It does so by facilitating regular problem resolution through the incorporation of daily changes in business norms and workforces. This reassures us about the effectiveness of AI in security technology.

[1] *How to cite the article:* Lamba S., (September 2023) Employability of Artificial Intelligence Algorithms for Enhancing the Effectiveness of Data Access Security Against Cyber Threats; *International Journal of Advanced Engineering*, Jul-Sep 2023, Vol 6, Issue 3, 30-36

Customer relationship management (CRM) is another vital component in business operations, enabling personnel to communicate with and update modifications based on customer perspectives. Both banking and non-banking institutions allocate capital resources to sustain sales and mass production to meet growing demand. Despite the plethora of services the Internet offers, including those for Internet of Things (IoT) users, communication infrastructure contends with various security and privacy risks, such as intrusion, replay attacks, identity theft, high complexity, insufficient resource utilization, and poor scalability.

AI can analyze data in real time to identify significant patterns, leading to insights that enhance knowledge bases, business strategies, and technological applications. Neural network-based diagnostic tools, in particular, excel in learning from prior data and updating their knowledge, surpassing other methods like expert systems and fuzzy logic. Additionally, the flexibility of neural networks enables the incorporation of inputs from field workers when new criteria emerge.

Furthermore, neural networks can elucidate interactions between input variables by ranking them to produce desired outputs, especially when the rules governing component interactions in a dataset are unclear. When analytical equations explaining input-output relationships are elusive, neural networks can predict outputs based on input variables.

Given the constant evolution of attacks on communication interfaces, cloud platforms, and vulnerabilities in hardware and software, defenders often need more prior knowledge of new attack modes and help to implement effective responses swiftly. Consequently, AI cybersecurity has garnered significant interest, not only among scientists but also everyday individuals. It addresses technical and scientific concerns and social and political implications.

Artificial intelligence encompasses various areas, including ordinary intelligence, computer vision, robotics, automated planning and scheduling, reasoning, and knowledge presentation. AI capabilities for self-configuration, tuning, management, healing, and diagnosis enable the development of automatic, context-aware computer solutions.

Looking ahead, AI studies focusing on bolstering cybersecurity measures in cyberspace appear promising. Given the escalating network threats and the need for robust security measures, the potential of AI in cybersecurity is undeniable. As AI becomes increasingly integrated into everyday activities, its role in information security is poised to expand further, offering innovative solutions to mitigate risks and enhance organizational resilience against cyber threats in the digital age. This instils confidence in the future of cybersecurity measures.

UTILIZING ARTIFICIAL INTELLIGENCE TO SAFEGUARD DATA ACCESS AGAINST CYBER THREATS

Figure 1 illustrates the integration of artificial intelligence into a security system as a flowchart. The process begins with the input block, which may include various sources such as historical data, technical requirements, real-time or offline reports, human inspections, assessment standards, occupational health and safety regulations, or client documents. Pre-processing is then applied to these inputs.

Users can then decide whether to retain or eliminate sensors by filtering out irrelevant inputs. This reduction in the number of sensors helps decrease hardware and communication costs. Additionally, leveraging distinct physical or behavioural traits for identifying individuals is discussed. Human identification and discernment between friends and foes are complex yet vital processes for survival. Humans typically authenticate the identity of others by analyzing their unique physical traits, belongings, or knowledge.

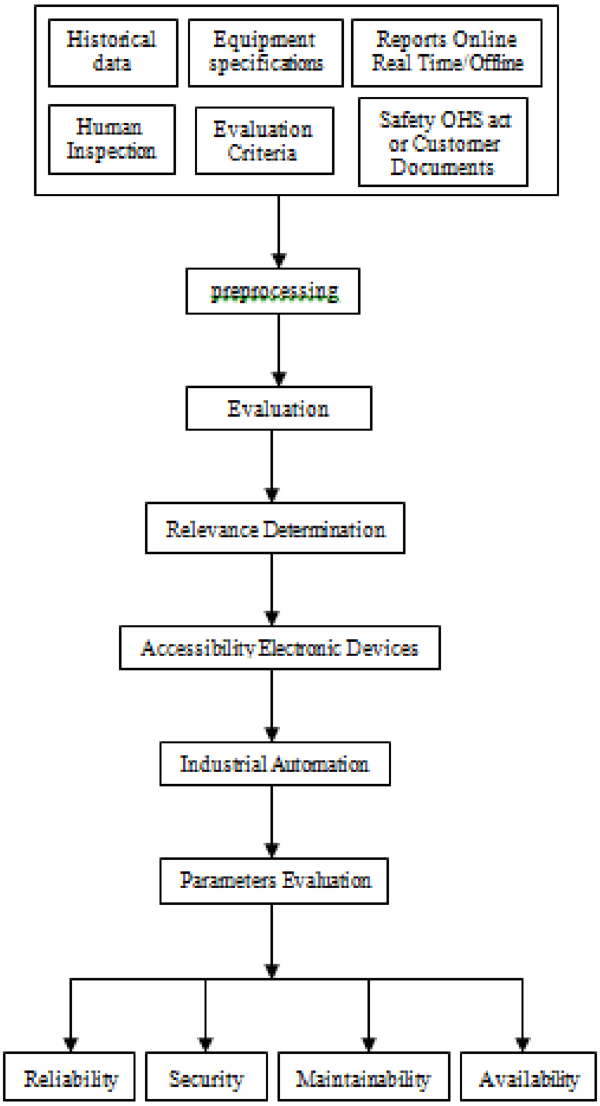


Fig. 1: Block diagram of Secure Data Access Management for Cyber Threats using Artificial Intelligence

Monitoring electronic device usage for accessing data is crucial to ensure service quality and meet customer needs. This requires the involvement of network architects, administrators, and ethical hackers to fortify systems against attacks. With a security system powered by artificial intelligence, these processes can be automated. Subsequently, parameter evaluation takes place.

Master control credentials are necessary to activate this algorithm upon its integration into an organization's network servers. Cloud storage facilitates streamlined utilization, strategy, and security management across different system layers. Data sharing among storage devices enhances accessibility in a multi-user environment.

The service layer offers a flexible means of delivering services and supporting platform-independent devices. Application programming interfaces provide various cloud storage system services tailored to user requirements for service management. Cloud technology enables users to access services via network-accessible storage, ensuring efficient service delivery.

RESULT ANALYSIS

This section presents the result analysis of secure data access management for cyber threats using artificial intelligence. Performance evaluation is based on the following definitions:

True Positive (TP): Correctly classified positive instances.

True Negative (TN): Correctly classified negative instances.

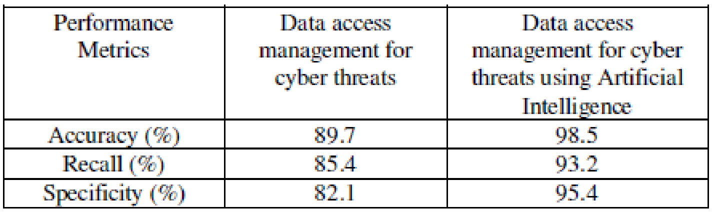
False Positive (FP): Incorrectly classified positive instances.

False Negative (FN): Incorrectly classified negative instances.

Accuracy, recall, and specificity metrics are calculated accordingly.

Table 1 illustrates the performance analysis of secure data access management for cyber threats using artificial intelligence. The results demonstrate superior accuracy, recall, and specificity, showcasing the effectiveness of this approach in securing data.

TABLE I. ANALYSIS OF PERFORMANCE



Performance Metrics	Data access management for cyber threats	Data access management for cyber threats using Artificial Intelligence
Accuracy (%)	89.7	98.5
Recall (%)	85.4	93.2
Specificity (%)	82.1	95.4

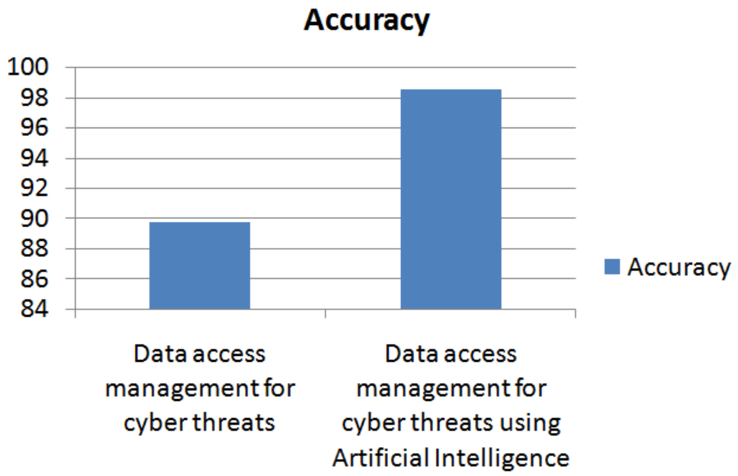


Fig. 2: Comparing the Accuracy Performance of Different Methods

Comparative analysis reveals that secure data access management for cyber threats employing artificial intelligence outperforms traditional methods, particularly in terms of recall and specificity.

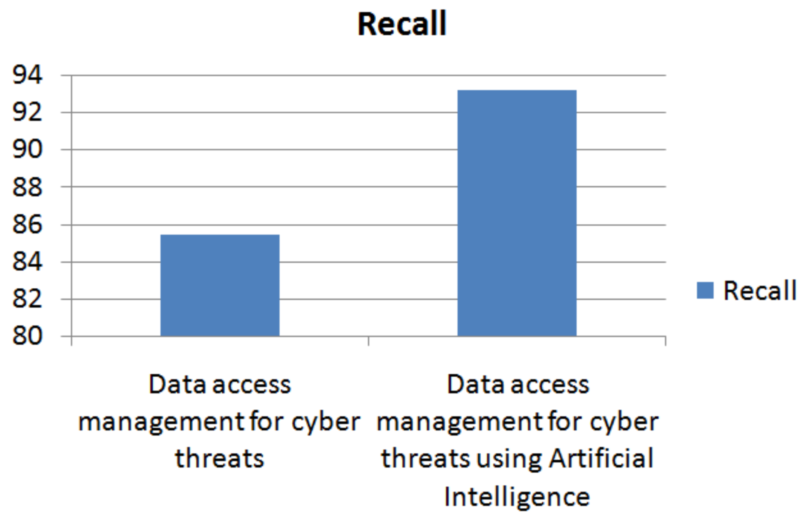


Fig. 3: Comparing the Recall Performance Across Methods

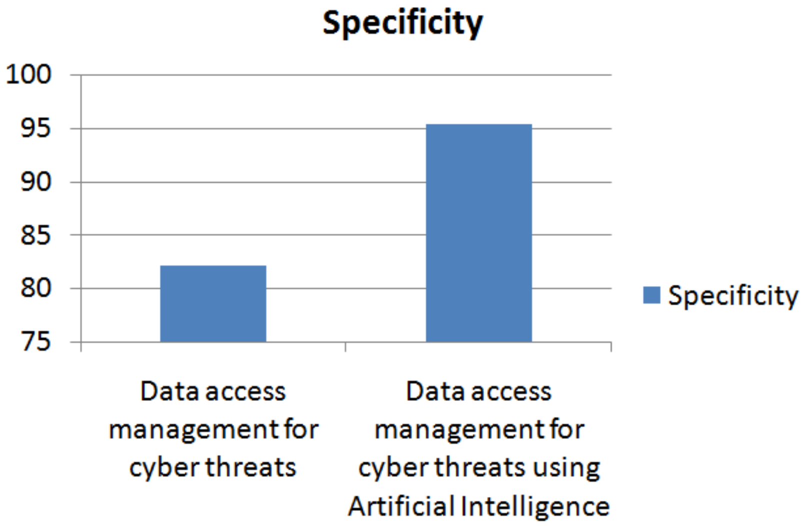


Fig. 4: Comparison of Specificity Performance Among Methods

CONCLUSION

The fragmented and non-standardized development of security technologies poses a significant challenge to their advancement. Integrating these technologies is cumbersome for users, emphasizing the need for detailed data security inspections.

Artificial intelligence emerges as a viable solution for enhancing data access management security. Its ability to handle complex computational tasks swiftly and accurately at a lower cost benefits enterprises seeking to safeguard sensitive data and assets.

The analysis of secure data access management for cyber threats using artificial intelligence confirms its efficacy in achieving high levels of accuracy, recall, and specificity. As cyber threats evolve, novel techniques like AI become indispensable for combating their increasing complexity.

REFERENCES

[1] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” ieee Commun. Surv. tutorials, p. 1, 2020, doi:10.1109/COMST.2020.2988293

[2] T.S. Tuang. Diep.Q. B, and Zelinka. I, Artificial Intelligence in the Cyber Domain: Offense and Defense: Symmetry, 2020, 12,410 available: www.mdp.com/journal/symmetry on [assessed Apr. 20, 2020]

[3] L. Lazic, Benefits from AI in Cyber Security, The 11th international Conference on Business Information Security, 18th Oct. 2019, Belgrade, Serbia, pp. 1-9

[4] S. Bhutada and P. Bhutada, Application of Artificial Intelligence in Cyber Security: in IJERCSE, 2018, 5(4): 214-219.

[5] S. A Panimalar, U.G. Pai and K.S. Khan, ―AI Techniques for Cyber Security, International Research Journal of Engineering and Technology, vol. 5, 3, pp. 122-124, Mar. 2018. Available: https://www.irjet.net [assessed May. 29, 2020]

[6] V. Esther Jyothi, Dr. BDCN Prasad, Dr. Ramesh Kumar Mojjada, “Analysis of Cryptography Encryption for Network Security”, IOP Conference Series: Materials Science and Engineering, DOI:10.1088/1757- 899X/981/2/022028, 2020.

[7] Smys, S., and Wang Haoxiang. "Data Elimination on Repetition using a Blockchain based Cyber Threat Intelligence." IRO Journal on Sustainable Wireless Systems 2, no. 4 (2021): 149-154.

[8] Madhuri, A., et al. "A New Multi-Level Semi-Supervised Learning Approach for Network Intrusion Detection System Based on the ‘GOA’." Journal of Interconnection Networks (2022): 2143047.

[9] S. Samonas and D. Coss, “The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security,” J. Inf. Syst. Secur., vol. 10, no. 3, pp. 21–45, 2014, [Online]. Available:http://www.proso.com/dl/Samonas.pdf.

[10] Sindhura, S., Praveen, S. P., Syedbi, S., Pratap, V. K., & Krishna, T. B. M. (2021). An effective secure storage of data in cloud using ISSE encryption technique. Annals of the Romanian Society for Cell Biology, 5321-5329.

[11] Praveen Phani Surapaneni *, Krishna Murali Thati Bala, Chawla Kumar Sunil and Anuradha Chokka, Virtual Private Network Flow Detection in Wireless Sensor Networks Using Machine Learning Techniques, International Journal of Sensors, Wireless Communications and Control 2021; 11(7) . https://dx.doi.org/10.2174/2210327910666210104160027

[12] Sindhura, S., Phani Praveen, S., Madhuri, A., Swapna, D. (2022). Different Feature Selection Methods Performance Analysis for Intrusion Detection.

[13] In: Satapathy, S.C., Bhateja, V., Favorskaya, M.N., Adilakshmi, T. (eds) Smart Intelligent Computing and Applications, Volume 2. Smart Innovation, Systems and Technologies, vol 283. Springer, Singapore.https://doi.org/10.1007/978-981-16-9705-0_51.

[14] E. H. Geoffrey, O. Simon and T. Yee-Whye, A Fast Learning Algorithm for Deep Belief Nets, Neural Computation, vol. 18, no. 7, pp. 1527-1554, 2006.