Threat Detection and Response Using AI and NLP in Cybersecurity

Dr. Walaa Saber Ismail[1*]

[1*]Assistant Professor, Business Information Technology Department, Liwa College, Abu Dhabi, UAE. walaa.saber@lc.ac.ae, https://orcid.org/0000-0002-4074-0156

Received: October 28, 2023; Accepted: December 30, 2023; Published: February 29, 2024

Abstract

Introduction: In an age of rapid technical innovation and a growing digital world, protecting sensitive data from cyberattacks is crucial. The dynamic and complicated nature of these attacks requires novel cybersecurity solutions.

Methods: This study analyses how Artificial Intelligence (AI) and Natural Language Processing (NLP) strengthen cybersecurity. The qualitative research approach is followed to gather data through a literature review of relevant scholarly articles and conduct interviews with cybersecurity specialists.

Results: Recent AI advances have greatly enhanced the detection of anomalous patterns and behaviors in huge datasets, a key threat identification tool. NLP has also excelled at detecting malevolent intent in textual data, such as phishing efforts. AI and NLP enable adaptive security policies, enabling agile responses to evolving security issues. Expert interviews confirm that AI and NLP reduce false positives, improve threat intelligence, streamline network security setups, and improve compliance checks. These technologies enable responsive security policies, which give a strategic edge against developing security threats. AI and NLP's predictive skills could revolutionize cybersecurity by preventing threats.

Conclusion: This study shows that AI and NLP have improved cybersecurity threat detection, automated incident response, and adaptive security policies. Overcoming threat detection, aggressive attacks and data privacy issues is essential to properly leveraging these advances and strengthening cyber resilience in a changing digital landscape.

Keywords: Cybersecurity, Artificial Intelligence (AI), Natural Language Processing (NLP), Behavioral Analysis, Anomaly Detection.

1 Introduction

The modern era is dominated by significant technological progress, the rise of new information, and an ever-expanding digital landscape. There is a critical need to protect sensitive data against the constant and escalating cyber threats. The changing and advancing nature of these risks, indicated by their increasing complexity and modification, requires the search of innovative solutions within the field of cybersecurity (Ustundag A, 2018). As a result of the present situation, Artificial Intelligence (AI) and

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 1 (February), pp. 195-205.
DOI: *10.58346/JISIS.2024.I1.013*

*Corresponding author: Assistant Professor, Business Information Technology Department, Liwa College, Abu Dhabi, UAE.

Natural Language Processing (NLP) are more important than ever before, and their potential for improving cyber security by enhancing threat detection and mitigation now gets clear (M. A.-R. , 2023; Chandana P, 2023).

Recent breakthroughs in artificial intelligence have greatly improved the ability to recognize anomalous patterns and behaviors within large datasets, a critical component of threat detection. The aforesaid improvements have facilitated the exceptional performance of machine learning algorithms in this particular field (Mishra A, 2020 ; Reddy DK, 2023). The NLP techniques have been crucial in enabling the detection of harmful intent in textual data, as demonstrated by their successful implementation in the identification of phishing efforts (Casino F, 2023). Scam detection using text has been greatly improved by NLP techniques successfully (Kumar S, 2023). AI also plays a crucial role in upgrading threat detection by employing text analysis techniques and automating incident assessment within the framework of incident response (Montasari R, 2021; Mazurek G, 2019). Therefore, the integration of AI and NLP has the capability to enable the development of adaptive security policies, thereby enable timely responses to emerging security threats (Wang J, 2021).

Moreover, the potential transformative impact of AI and NLP in the field of threat prevention lies in their predictive capabilities, which enable the anticipation of possible cyber threats before they materialize (Aziz LA, 2023 ; Aziz LA, 2023 ; M. B. , 2021 ; Ahmad A, 2023). The purpose of this study is to examine the use of AI and NLP in the perspective of cyber security. It will help us to figure 1 out how AI and NLP can change the world and what that means for the future of cyber security.

2 Aim of the Study

This study aims to assess the efficacy of AI and NLP for detecting cyber threats.

Questions

Q1: How AI and NLP technologies effectively enhance threat detection of cyber threat landscape?

Q2: How to assess the role of AI and NLP in automating incident triage and incident response processes in cyber security?

Q3: How can the integration of AI and NLP facilitate the development of adaptive security policies for responsive actions against evolving security risks?

3 Methods

Research Data

This is a qualitative research approach to investigate the impact of AI and NLP on Cybersecurity. The data was gathered from multiple sources, including social media platforms, websites, the healthcare sector, and banks, and confirmed by cybersecurity experts through interviews. The data was collected from previous research articles and expert interviews with their practical expertise that ratify the importance of both AI and NLP for cybersecurity.

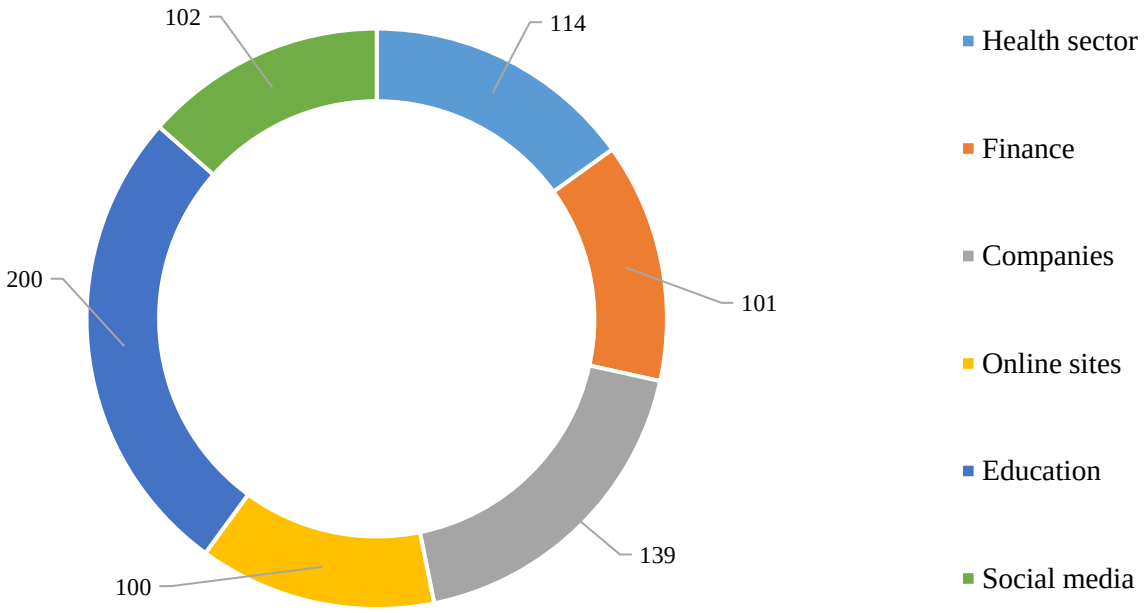

Figure 1: Data collection of different platforms to check the AI and NLP use in these organizations

Data Collection

The process of data collecting starts with an extensive examination of relevant literature derived from scholarly articles about the health sector, finance and industry, social media, and online sites (Table 1). Then a comprehensive collection of relevant materials was research papers related to the fields of AI, NLP, and cybersecurity was compiled.

Survey

A series of in-depth interviews were conducted with cybersecurity specialists who worked in the selected organizations. The interviews were conducted online to ease accessibility and arrangement. The main purpose of conducting these interviews was to acquire significant perspectives on the practical applications of AI and NLP in boosting digital security practices to prevent cyber-attacks.

Arrangement of Data

Thematic analysis was used to explain fundamental concepts, perceptions, and patterns pertaining to the convergence of AI and NLP within the domain of cybersecurity. Milvus database was used to analyze the data through different steps. The textual content extracted from various sources undergoes a rigorous process of systematic analysis to identify and interpret significant findings. The final application was then confirmed by the experts with their practical implementation and valuable experience.

Table 1: Data processing and optimization

Step	Description
1.	Data Collection: Gather data from various sources, including logs, network traffic, and system events.
2.	Data Preparation: Clean, format, and transform raw data to make it suitable for future analytical processes.
3.	Feature Extraction: Extract relevant features from pre-processed data for input into AI and NLP models.
4.	Data Analysis: Conduct a comprehensive examination of data to identify patterns, trends, and anomalies that may indicate potential threats.
5.	Machine Learning and NLP Models: Utilize AI and NLP models to process and analyze data in a sophisticated manner, aiding in the detection of abnormal behavior and linguistic patterns.
6.	Prediction: Proactively identify and assess potential hazards and vulnerabilities using machine learning and NLP algorithms to generate outcomes.
7.	Alert Generation: Generate alerts or notifications when potential hazards or anomalies are detected.
8.	Hazard Verification: Automate operations to confirm the existence of recognized hazards through inquiries.
9.	Mitigation Measures: Implement measures to mitigate issues, including segregating affected systems, applying security fixes, or modifying configurations.

4 Results

Q1: How do AI and NLP technologies effectively enhance threat detection of the cyber threat landscape?

Enhanced Anomaly Detection: Machine learning algorithms have recently made major strides in AI, which have considerably enhanced our ability to detect abnormal patterns and behaviors in huge datasets. This has increased the efficiency of anomaly-based threat detection and made it possible to identify sophisticated threats that were previously unidentified (Table 2). AI can keep up with changing threats thanks to its capacity to adapt and learn from fresh data over time (Himeur, 2021).

Effective Text Analysis: NLP methods have been shown to be essential in spotting malicious intent in text. An application worth mentioning is the accurate detection of phishing efforts, where NLP systems excel at understanding the language traits of bogus emails. Text analysis has been greatly enhanced by NLP approaches in terms of scam detection (Liu. B, 2022 May 31).

Automated Incident Evaluation: Within the context of incident response, AI is essential for automating incident evaluation. AI systems can quickly determine the seriousness of a security event and take the necessary action by evaluating textual data and other pertinent information, which speeds up response times and boosts overall security (Kaur R, 2023; Pan Y, 2021).

Reduction of false positives: NLP techniques have been incorporated, which has decreased the number of false positive alerts. NLP assists in filtering out irrelevant warnings, reducing the workload on security personnel and enabling them to concentrate on real risks by considering the linguistic context and intent underlying security occurrences (Hegedűs P, 2022).

Adaptive Security Policies: AI and NLP working together could make it possible to create these security policies. In contrast to NLP, which aids in comprehending the linguistic context of security incidents, AI can continuously learn and adapt to new threats. This collaboration may result in security solutions that are more responsive and adaptable to new threats in real time (Usama M, 2021).

Predictive skills: AI and NLP technologies provide predictive skills that allow for the early detection of cyber threats (Ahmed I, 2022). These tools can issue early warnings about prospective hazards by assessing historical data, patterns, and linguistic clues. AI and NLP have improved the dynamic cyber threat scene. Adaptive security rules, automated incident evaluation, text analysis, anomaly detection, and false positive reduction are greatly improved by these technologies. Their predictive powers enable pre-emptive threat identification. Domain knowledge, data privacy, and adversarial attacks must be addressed for these technologies to improve cybersecurity (Wong and Yiu 2020).

Table 2: Practical Applications of AI and NLP in Cyber Security

Application	Description	Example	Impact
Threat Detection	AI-driven anomaly detection algorithms for identifying suspicious patterns in login attempts, enabling early risk mitigation.	The financial institution identifies a sophisticated attack based on login patterns and prevents data breaches.	Prevention of potential data breaches and financial losses.
Malicious Intent Recognition	NLP-based analysis of textual data, such as patient records, to detect unauthorized access and protect confidentiality.	Healthcare organization identifies an employee attempting unauthorized access to medical data.	Safeguarding patient confidentiality and data privacy.
Phishing Detection	NLP is used to analyse email content, identifying phishing attempts missed by traditional filters through language clues.	Software company detects previously unnoticed phishing emails.	Prevention of unauthorized data access and safeguarding sensitive information.
Behavioural Analysis	AI-driven analysis of user behavior to detect insider threats and unusual data access behaviour, proactively protecting sensitive information.	Government organization detects insider threat trying to steal government data.	Safeguarding national security and preventing data breaches and insider threats.

Q2: How to assess the role of AI and NLP in automating incident triage and incident response processes in cyber security?

Effective Incident Triage: It has been shown that AI-driven incident triage systems are quite effective in quickly classifying and prioritizing security events. AI can assess the severity and context of incidents by assessing a variety of data sources, including as log files and network traffic. This streamlines the triage process and guarantees that the most urgent risks are dealt with right away (Mohanty S, 2018).

Text Analysis for Security Incident Identification: NLP technologies have shown their efficacy in automating the detection of security incidents through text analysis. Included in this is the identification of malevolent intent in textual data, such as the recognition of phishing emails using linguistic patterns. By quickly highlighting possible hazards, NLP-driven incident detection shortens reaction times (Whig P, 2023 Aug 4).

Incident response of AI: Based on the analysis of incident data, it might suggest reaction plans or carry out specified actions. For example, AI solutions can isolate hacked systems or automatically block suspicious IP addresses to lessen the impact of an incident in real-time (Chandana P, 2023).

Contextual knowledge: By giving us a better knowledge of the language context of situations, NLP improves incident response. This makes it possible for security teams to determine the purpose and

source of attacks more accurately, enabling more precise and focused responses. NLP-driven incident response reduces false positives and makes sure that the replies match the incident's nature (Liu. B, 2022 May 31).

Faster Resolution: Using AI and NLP technology to automate incident response, incidents are resolved more quickly. Security incidents can be less harmful when automated actions, including limiting malicious activity or quarantining compromised devices, are carried out quickly (Evans HP, 2020).

Reduction in Human Error: Using AI and NLP to automate incident triage and response processes reduces the possibility of human error. The technologies can accurately and reliably process enormous amounts of data, which lessens the need for manual intervention and boosts the overall effectiveness of security operations (Wilson L, 2022). The critical factors to ensure the successful adoption of these technologies include ensuring that the systems have access to the most recent threat intelligence, addressing the possibility of adversarial attacks on AI models, and maintaining privacy compliance (Salloum S, Jan). These innovations have the potential to increase cyber resilience and lessen the effects of security incidents. To fully realize the advantages of these technologies in incident response, it is necessary to solve issues with threat intelligence, adversarial attacks, and data privacy.

Q3: How can the integration of AI and NLP facilitate the development of adaptive security policies for responsive actions against evolving security risks?

Learning Adaptation: Systems based on artificial intelligence are capable of continuously learning about security concerns and adapting to them. It prevents new threats, and machine learning algorithms by assessing changing threat patterns, finding anomalies, and modifying security rules in real time (Baidoo-Anu D, 2023).

Better Threat Detection: The language context, behaviour, as well as intent, AI and NLP help to identify threats more accurately. For instance, NLP aids in comprehending the language used in security incidents, improving risk assessment, and enabling the creation of precisely tailored security policies (Reddy DK, 2023; Wilson L, 2022).

Quick and Real Response: Real-time reactions to security incidents are made possible by the union of AI and NLP. Security policies can quickly change to mitigate threats as they arise by automating the analysis of event data and providing appropriate responses depending on the context (Azaria A, 2014).

Reduced False Positives: By giving a richer understanding of the incident context, NLP technology can drastically minimize false positive alarms by using their linguistic analysis skills. The effectiveness of policy responses is increased by the decrease in false positives, which allows security teams to concentrate on real risks (Ahmed I, 2022 ; Liu. B, 2022 May 31).

Access Adaptive Control: Access controls can be dynamically changed based on user behaviour with adaptive access control, a feature of AI-powered systems. The potential impact of hacked accounts or insider threats can be reduced by these systems' ability to identify irregularities in user behavior and respond by altering access rights (Evans HP, 2020).

Defensive Threat Mitigation: Proactive Threat Mitigation is a possibility made possible by AI and NLP technology. These systems can foresee and anticipate security problems by assessing historical data, enabling the creation of preventative security policies and actions (T., 2023). Despite the obvious benefits, there are obstacles to overcome in the integration of AI and NLP for adaptive security policies. These include worries about domain expertise, the requirement for ongoing AI model updates to stay abreast of new security threats, and the possibility of hostile AI system attacks (Chandana P, 2023; Kaur

R, 2023). AI and NLP help create adaptive security rules to address changing security threats. These technologies provide proactive threat mitigation, real-time replies, fewer false positives, continuous learning, and enhanced threat detection. Domain knowledge, model updates, and adversarial attacks must be addressed to employ AI and NLP to create adaptive security policies.

Interviews Outcomes

The nnotable findings of interviews reveal that AI and NLP technologies have had a positive impact on digital security (Table. 3). These innovations have reduced false positives in incident response, enhanced the detection of phishing and social engineering attacks, improved threat intelligence, streamlined network security configurations, and aided in compliance checks, among other benefits.

Table 3: Survey Responses from Cybersecurity Specialists

No. P	Experience (Years)	Organization	AI Integration (Scale 1-5)	NLP Integration (Scale 1-5)	Security Efficacy Improvement (%)
20	2-8	Social Media	4	3	35
25	3-12	Health Sector	3	2	47
31	4-5	Finance	5	4	25
14	5-10	Online website	4	3	36
08	15	Industry	5	4	50

5 Future Prospects and Recommendations

The potential of AI and NLP in cyber security was discussed in detail by industry experts. They hypothesized that businesses would be able to better deal with constantly shifting security threats if they adopted responsive security policies made possible by combining the aforementioned technologies. The predictive capacities of AI and NLP were also viewed as a game-changer, with the potential to enable proactive threat prevention.

6 Discussion

The findings showed how AI and NLP technology improve threat detection, automate incident triage and response, and help cybersecurity policymakers create adaptive security policies.

Improved Threat Detection

The first research question (Q1) examined how AI and NLP improve threat detection. Results show that AI, especially machine learning algorithms, has greatly improved anomaly-based threat identification. It adapts to developing threats to identify previously unknown complex attacks. These findings match previous research (Himeur, 2021). NLP approaches excel in text analysis, allowing precise identification of harmful intent in diverse circumstances, such as phishing efforts (Liu. B, 2022 May 31).

Triage and Response Automation

Q2 examined how AI and NLP automate incident triage and response. The results showed that AI-driven incident triage systems categorize and prioritize security incidents, speeding up urgent risk response (Mohanty S, 2018). However, NLP has led to automated security event identification using text analysis, including malicious intent (Whig P, 2023 Aug 4). Previous research has shown that AI and NLP improve response speeds, contextual knowledge, and incident resolution (Wilson L, 2022). To successfully use these technologies, threat intelligence, adversarial attacks, and data privacy must be addressed (Usama M, 2021; T., 2023).

Protected Policies That Change

The third research question (Q3) examined AI-NLP integration for adaptive security strategies. Results show that AI's learning adaptation and NLP's linguistic context comprehension increase threat detection and enable customized security policies (Mohanty S, 2018). AI and NLP enable real-time security incident response, false positive reduction, and adaptive access control (Baidoo-Anu D, 2023). These findings support research on AI and NLP's abilities to prevent security threats and improve security policy flexibility (T., 2023 ; Leone D, 2021).

Security Expert Opinion

Cybersecurity expert interviews provided real-world insights. The comments showed how AI and NLP affect digital security. These solutions reduced false positives, improved threat intelligence, streamlined network security configurations, and helped compliance checks by detecting phishing and social engineering attempts. The survey results support the research, showing that AI and NLP can solve cybersecurity problems across disciplines (Fernandes G, 2019; Saeed S, 2023).

7 Future Prospects and Suggestions

Interviews with industry experts highlighted AI and NLP's cybersecurity possibilities. These technologies provide responsive security policies, which should help corporations respond to changing security threats (Koleck TA, 2019; R., 2021). AI and NLP's predictive powers could revolutionize cybersecurity by enabling proactive attack avoidance. This recommends that organizations should continue to invest in research and development in these areas while also tackling major concerns including updated threat intelligence, AI model adversarial attacks, and data privacy compliance. The overviews of cybersecurity experts reveal that AI and NLP technologies have improved threat detection, incident response automation, and adaptive security policies in cybersecurity. Further breakthroughs in these areas could give organizations new tools and tactics to combat growing cyberthreats.

8 Conclusion

New insights from this study highlight the importance of AI and NLP in enhancing network security. The research confirms that the adaptive learning capabilities of AI, the language context comprehension of NLP, and the combination of the two offer substantial improvements in threat detection, incident response automation, and the creation of adaptive security policies. According to experts in the field, these solutions help lower false positive rates, speed up incident resolution, and arm businesses with the resources they need to proactively counteract the growing threats to their information security. These technologies provide the foundation for responsive security policies that will allow for more nimbleness in the face of evolving threats. AI and NLP's predictive powers are also essential for stopping threats before they even happen. Achieving full utilization of these advantages requires fixing problems with threat intelligence, adversarial attacks, and data privacy. Organizations may greatly improve their cyber resilience by continuing to engage in these advances and tackling their issues, protecting their data and assets in the digital realm.

9 Ethical Considerations

Ethical approval was taken from all participants before the interviews. The participant anonymity and data confidentiality were ensured to help out similar research in the future.

10 Limitations

The limitations include the availability and reliability of cyber security incident data and potential biases in survey responses.

11 Recommendations

It is recommended to optimize AI/NLP integration in cyber security practices and for future research in the field.

12 Conflict of Interest

There is no conflict of interest in the current research.

References

[1] Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. *Eigenpub Review of Science and Technology*, *7*(1), 138-158.

[2] 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: Multidisciplinary Journal of Science*, *2*(2), 443-455.

[3] Ahmed, I., Jeon, G., & Piccialli, F. (2022). From artificial intelligence to explainable artificial intelligence in industry 4.0: a survey on what, how, and where. *IEEE Transactions on Industrial Informatics*, *18*(8), 5031-5042.

[4] Azaria, A., Richardson, A., Kraus, S., & Subrahmanian, V.S. (2014). Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. *IEEE Transactions on Computational Social Systems*, *1*(2), 135-155.

[5] Baidoo-Anu, D., & Ansah, L.O. (2023). Education in the era of generative artificial intelligence (AI): Understanding the potential benefits of Chat GPT in promoting teaching and learning. *Journal of AI*, *7*(1), 52-62.

[6] Belk, R. (2021). Ethical issues in service robotics and artificial intelligence. *The Service Industries Journal*, *41*(13-14), 860-876.

[7] Bing, L. (2022). Sentiment analysis and opinion mining. https://books.google.com.pk/books?hl=en&lr=&id=xYhyEAAAQBAJ&oi=fnd&pg=PP1&dq=Effective+Text+Analysis:+NLP+methods+have+been+shown+to+be+essential+in+spotting+malicious+intent+in+text.+&ot

[8] Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review*, *81*(5), 825-836.

[9] Casino, F., Totosis, N., Apostolopoulos, T., Lykousas, N., & Patsakis, C. (2023). Analysis and correlation of visual evidence in campaigns of malicious office documents. *Digital Threats: Research and Practice*, *4*(2), 1-19.

[10] Dash, B., Sharma, P., & Ali, A. (2022). Federated learning for privacy-preserving: A review of PII data analysis in Fintech. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(4), 13401. https://doi.org/10.5121/ijsea.2022.13401

[11] Evans, H.P., Anastasiou, A., Edwards, A., Hibbert, P., Makeham, M., Luz, S., & Carson-Stevens, A. (2020). Automated classification of primary care patient safety incident report content and severity using supervised machine learning (ML) approaches. *Health informatics journal*, *26*(4), 3123-3139.

[12] Fernandes, G., Rodrigues, J.J., Carvalho, L.F., Al-Muhtadi, J.F., & Proença, M.L. (2019). A comprehensive survey on network anomaly detection. *Telecommunication Systems*, *70*, 447-489.

[13] Hassan, M., Aziz, L.A.R., & Andriansyah, Y. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

[14] Hegedűs, P., & Ferenc, R. (2022). Static code analysis alarms filtering reloaded: A new real-world dataset and its ML-based utilization. *IEEE Access*, *10*, 55090-55101.

[15] Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F., & Amira, A. (2021). Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives. *Applied Energy*, *287*, 116601. https://doi.org/10.1016/j.apenergy.2021.116601

[16] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[17] Koleck, T.A., Dreisbach, C., Bourne, P.E., & Bakken, S. (2019). Natural language processing of symptoms documented in free-text narratives of electronic health records: a systematic review. *Journal of the American Medical Informatics Association*, *26*(4), 364-379.

[18] Kumar, S., Gupta, U., Singh, A.K., & Singh, A.K. (2023). Artificial intelligence: revolutionizing cyber security in the digital era. *Journal of Computers, Mechanical and Management*, *2*(3), 31-42.

[19] Leone, D., Schiavone, F., Appio, F.P., & Chiao, B. (2021). How does artificial intelligence enable and enhance value co-creation in industrial markets? An exploratory case study in the healthcare ecosystem. *Journal of Business Research*, *129*, 849-859.

[20] Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344-364.

[21] Mishra, A., & Yadav, P. (2020). Anomaly-based IDS to detect attack using various artificial intelligence & machine learning algorithms: a review. *In 2nd International Conference on Data, Engineering and Applications (IDEA)*, 1-7.

[22] Montasari, R., Carroll, F., Macdonald, S., Jahankhani, H., Hosseinian-Far, A., & Daneshkhah, A. (2021). Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. *Digital Forensic Investigation of Internet of Things (IoT) Devices*, 47-64.

[23] Pan, Y., & Zhang, L. (2021). Roles of artificial intelligence in construction engineering and management: A critical review and future trends. *Automation in Construction*, *122*, 103517. https://doi.org/10.1016/j.autcon.2020.103517

[24] Pandem, C., & Mohammed, G.C. (2023). Securing Cyberspace: A Comprehensive Journey through AI's Impact on Cyber Security. *Tuijin Jishu/Journal of Propulsion Technology, 44*(2). 182-196.

[25] Reddy, D.K., Behera, H.S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P.K. (2021). Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. *Transactions on Emerging Telecommunications Technologies*, *32*(7), e4121. https://doi.org/10.1002/ett.4121

[26] Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H., & Almuhaideb, A.M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

[27] Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using natural language processing techniques: a literature survey. *Procedia Computer Science*, *189*, 19-28.

[28] Soumendra, M., & Sachin, V. (2018). Cybersecurity and AI. How to Compete in the Age of Artificial Intelligence. *Implementing a Collaborative Human-Machine Strategy for Your Business*, 143-53.

[29] Tim, H. (2023). Explainable Artificial Intelligence (XAI): Concepts and Challenges in Healthcare. *Artificial Intelligence*, *4*(3), 652-666.
[30] Usama, M., Mokhlis, H., Moghavvemi, M., Mansor, N.N., Alotaibi, M.A., Muhammad, M.A., & Bajwa, A.A. (2021). A comprehensive review on protection strategies to mitigate the impact of renewable energy sources on interconnected distribution networks. *IEEE Access*, *9*, 35740-35765.
[31] Ustundag, A., Cevikcan, E., Ervural, B.C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. *Industry 4.0: managing the digital transformation*, 267-284.
[32] Wang, J., Wang, X., Ma, C., & Kou, L. (2021). A survey on the development status and application prospects of knowledge graph in smart grids. *IET Generation, Transmission & Distribution*, *15*(3), 383-407.
[33] Whig, P., Velu, A., Nadikattu, R.R., & Alkali, Y.J. (2023). Computational Science Role in Medical and Healthcare-Related Approach. *Handbook of Computational Sciences: A Multi and Interdisciplinary Approach*, 245-272.
[34] Wilson, L., & Marasoiu, M. (2022). The development and use of chatbots in public health: scoping review. *JMIR human factors*, *9*(4), e35882. https://doi.org/10.2196/35882
[35] Wong, S.K., & Yiu, S.M. (2020). Location spoofing attack detection with pre-installed sensors in mobile devices. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *11*(4), 16-30.

Author Biography

Dr. Walaa Saber Ismail, Ph.D. in computer science and information systems. She possesses significant expertise in educational instruction and administrative leadership within higher education. Her academic focus revolves around Natural Language Processing, Sentiment Analysis, Machine Learning, Information Security and Business Analytics. She participates as a reviewer for various international peer-reviewed journals and fulfills roles as a program committee member for multiple national and international conferences. Currently, she holds the position of head of the Business Information Technology department at Liwa College.