Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Advanced Machine Learning Techniques for Cybersecurity: Enhancing Threat Detection in US Firms

Mita Khatun[1]✉ Mahjabin Siddika Oyshi[2]
[1]Department of Building Engineering and Construction Management, Khulna University of Engineering & Technology, Khulna, Khulna-9203, Bangladesh.
[2]Department of Statistics, Shahjalal University of Science and Technology, Kumargaon, Sylhet-3114, Bangladesh
Corresponding Author: Mita Khatun **E-mail**: mitakhatun1923028@gmail.com

| ABSTRACT

US corporations' computing technologies are evolving towards new technologies to detect, respond, and prevent new threats using sophisticated machine learning (ML) methods for their cybersecurity systems. To be sure, machine learning is not a silver-bullet solution, but it does have speed, scalability, and pattern detection capacity which have no match. Robust cybersecurity is built on a multi-faceted strategy incorporating cutting-edge machine learning models with traditional countermeasures and human expertise. By collaborating, engineers, legislators lawyers can ensure safe and responsible execution in business, especially in the high-stakes world of US companies. This paper describes how machine learning (ML) can enhance threat detection systems, enabling enterprises to move from reactive to proactive defense strategies. But beyond the effectiveness of the technologies, we emphasize the need for accountability, transparency and ethical governance in deploying these technologies. Finding the right spot for the combination of machine learning's computational capabilities without abandoning decisions because of any relationship remains part of ethical assessment and passive strategy. But, as attacks become more complex, we need our defenses to do the same. However, this study uses the power of machine learning to study more and implement it correctly so US companies can create a resilient and agile cybersecurity solution that will safeguard their digital assets in an increasingly interconnected world.

| KEYWORDS

Advanced machine learning, cybersecurity, threat detection, US firms, supervised learning, data security, predictive analytics, real-time monitoring.

| ARTICLE INFORMATION

ACCEPTED: 19 March 2025 **PUBLISHED:** 23 April 2025 **DOI:** 10.32996/jcsts.2025.7.2.31

1. Introduction

With the rapid expansion of digital platforms and the growing complexity of cyber threats, cybersecurity has become more important than ever before (Imran et al., 2024; Manoharan & Sarker, 2023). It is essential in shielding from these challenges while ensuring a degree of personal privacy, shielding organizations, preventing economic loss, and maintaining public safety (Bhuiyan et al., 2025a). One of the major developments coming into the realm of cybersecurity is the emergence of Artificial Intelligence (AI) as a game-changer (Ahmed et al., 2025; Mohamed, 2023). AI provides better results than previous security systems. AI puts those skills to use when it comes to processing massive data sets, learning through experience, and predicting future threats with high accuracy (N. N. Islam Prova, 2024b). Thus, making it a serious component of Cybersecurity protocols (Das et al., 2023). The digital transformation has also brought many challenges into play, especially in the area of cybersecurity. Traditional security tools such as antivirus programs and firewalls are not able to keep up with an evolving and ever more sophisticated cyber threat landscape (M. A. Islam et al., 2025; R. Kaur et al., 2023). The demand for dynamic, robust, and effective cybersecurity solutions continues to rise (Johora et al., 2024). In this scenario, the rise of AI in cybersecurity has the potential to revolutionize the sector (Goffer et al., 2025). AI, which is proficient at replicating and even outperforming human cognitive functions, is considered a significant element in bolstering cybersecurity. Leveraging complex algorithms, AI and machine learning are able to detect patterns through large datasets, learn from new data, and predict threats with considerable accuracy (M. Islam et al., 2025). Its high speed and accuracy, as well as its ability to identify new cyber threats, far outstrip those of traditional security systems, making it an increasingly important component of cybersecurity protocols (Ahmed et al., 2023; Schmitt et al., 2023). Fig. 1 shows a cybersecurity model.

Fig. 1. A cybersecurity model

2. An overview of common cybersecurity attacks

In cyberspace, hackers, cybercriminals, and other online enemies use different types of techniques for an attack (J. Kaur et al., 2023). Their primary objective is to gain access to data in computer networks or systems without authorization, sometimes with the intention of modifying, degrading or publicizing confidential information (N. N. I. Prova, 2024). These hacks can have businesses, people or even the government in their crosshairs (Kamal et al., 2025; Vacca, 2013). The rise of these assaults has underscored the urgent demand for enhanced cybersecurity defense mechanisms, leading to the development of advanced solutions such as machine learning (ML) and artificial intelligence (AI) (Hasan et al., 2025; Hossain et al., 2024). Fig. 2 shows cyberattack trends (T. Akter et al., 2024; N. N. Islam Prova, 2024a).

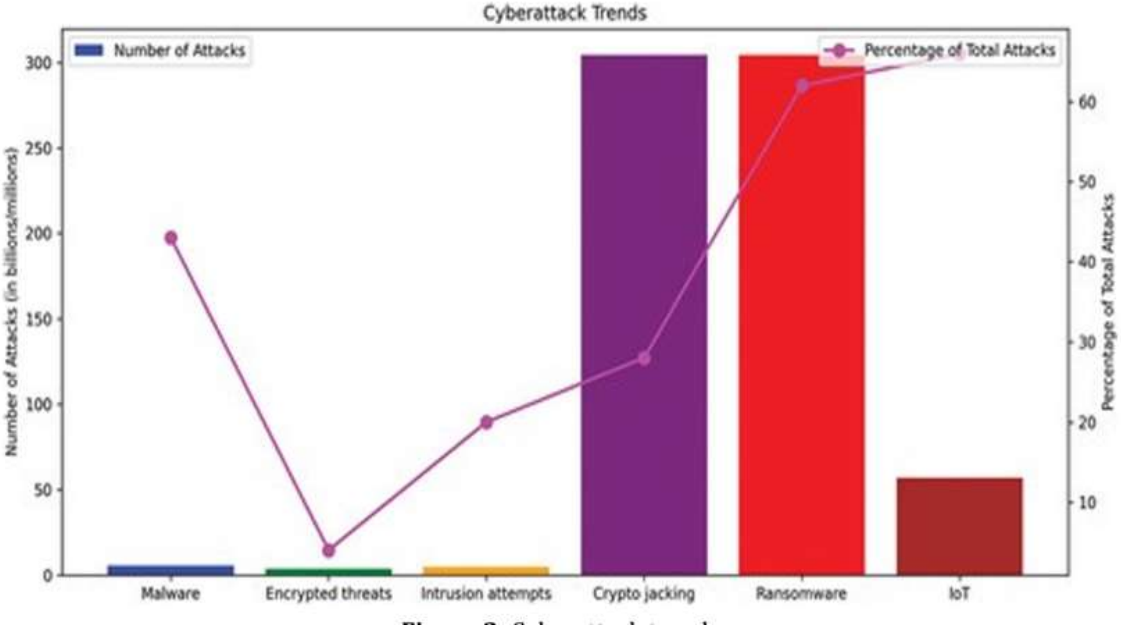

Fig. 2. Cyberattack trends

2.1 Malware

Malware, which encompasses ransomware, trojans, spyware, viruses, worms, keyloggers, bots and crypto jacking, is the most frequent type of attack in cyberattacks at 43% of all attacks (Mahmud et al., 2025; Manik et al., 2025). Following this, the second most common type is intrusion attempts, then it is followed by: ransomware (61%), crypto jacking (29%), encrypted threats and Internet of Things (69%) (Capuano et al., 2022; Khair et al., 2025).

2.2. Denial of service (DoS) attacks

These types of attacks undeniably serve providers for the Request overload network, causing disruptions to corporations and removing users ' use of, Web websites, online accounts, and e-mail. While it does not lead to loss of data, it is costly for organizations. Distributed Denial of Service (DDoS) assaults are tougher to stop (Md Ekrim et al., 2024).

2.3. Phishing

Phishing is a kind of cyber assault through which victims are duped into giving up personal information using social engineering, cellphone calls, SMS and emails (Kamruzzaman et al., 2024). The other types, such as supply chain attacks, code injection attacks, identity-based attacks, and spoofing, further highlight the nature of cyber threats evolving constantly (Md Habibullah Faisal, 2022).

2.4. Challenges in traditional threat detection methods

Conventional threat detection methods face challenges in maintaining system and network security due to the ever-evolving threat landscape, evolving hackers, and the need for periodic upgrades (Mia Md Tofayel Gonee et al., 2020). New threats require detection methods to be refined, processes to be monitored, and incidents addressed quickly, a triple whammy that can stretch staff and resources (J. Kaur et al., 2023).

2.5. Limitations:

The joint efforts of them using rules-based cybersecurity platforms Y and Z do not yield a complete picture due to challenges with manual data correlation, extraction, siloed insights, and an inability to visualize network behavior in real-time (Ferdousmou et al., 2025). Both solutions lead to increased technological and architectural complexity with hybrid solutions, while legacy cybersecurity is struggling to keep pace with the massive scale and complexity. As its consequences can give rise to the loss of money, sensitive information, and reputation, finding better solutions in cybersecurity becomes paramount. Fig. 3 shows AI-based vs traditional security threat detection (Debnath et al., 2024).

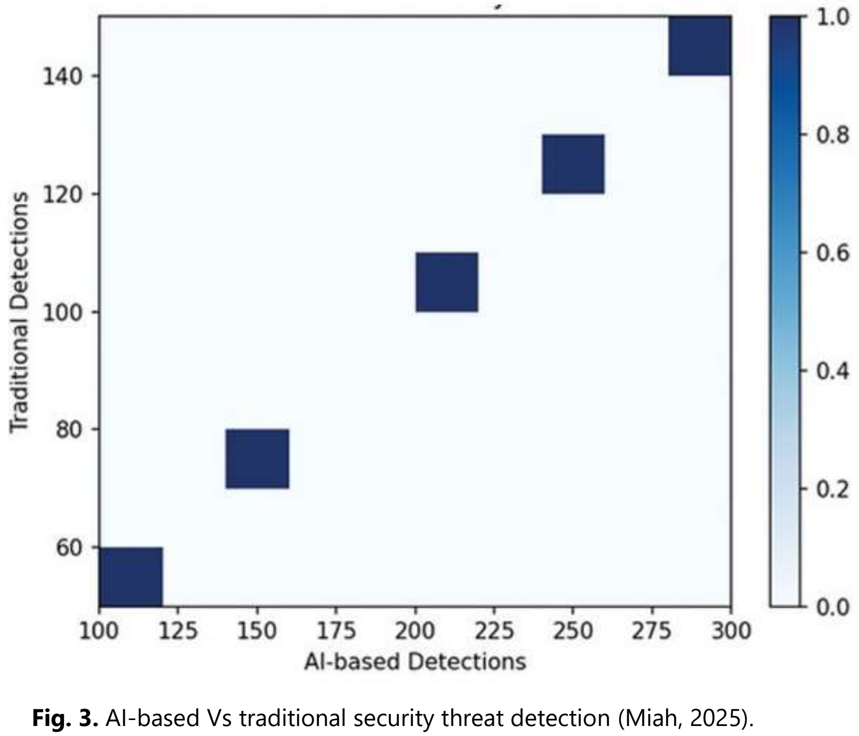

Fig. 3. AI-based Vs traditional security threat detection (Miah, 2025).

3. Methodology

Artificial intelligence and machine learning technologies have drastically improved network security by detecting and preventing threats such as DDoS, unauthorized infiltration, and Advanced Persistent Threat (APT) attacks more accurately and efficiently (Mohammad Abdul et al., 2024; Niropam Das 2025). They can also be used for threat intelligence, management, and security automation (Saimon et al., 2023).

3.1 Identify

The identity function is a critical element of cybersecurity, uncovering vital functions and threats around the people, assets, data, and systems (Bhuiyan et al., 2025b). It helps businesses understand their cybersecurity posture on the current day, determine large areas of concern, and develop a risk management approach that meets their particular requirements, vulnerabilities, and spending plan. In this role, they utilize cybersecurity solutions such as asset management, asset inventory management, business environment, and automated business impact analysis. Asset management requires finding and tracking things in an organization that support its goals, such as people, data, facilities, systems, and equipment. AI-equipped asset management systems can help in mitigating these by providing complex intelligence. Asset inventory management protects your complete assets by ensuring total view and control over assets both inside and outside in an extended network, which helps in preventing any security flaws and reduces the risk of them accessing any of your data (Chowdhury et al., 2023; Das et al., 2023). The business environment category describes the critical processes and tools to keep your company up and running during tough times (Khair et al., 2025). By putting AI technology to work, this process can be automated, and its accuracy and efficiency would see a significant boost. Automated business impact analysis is one of the key techniques for identifying critical operations and apps in the corporate environment, and for assessing the potential effects of cyber events. By leveraging AI, organizations can enhance the effectiveness and precision of their business impact analyses, ultimately streamlining their cybersecurity activities and enabling sound decision making. Fig. 4 shows AI/ML usage in security automation (Biswas et al., 2024).

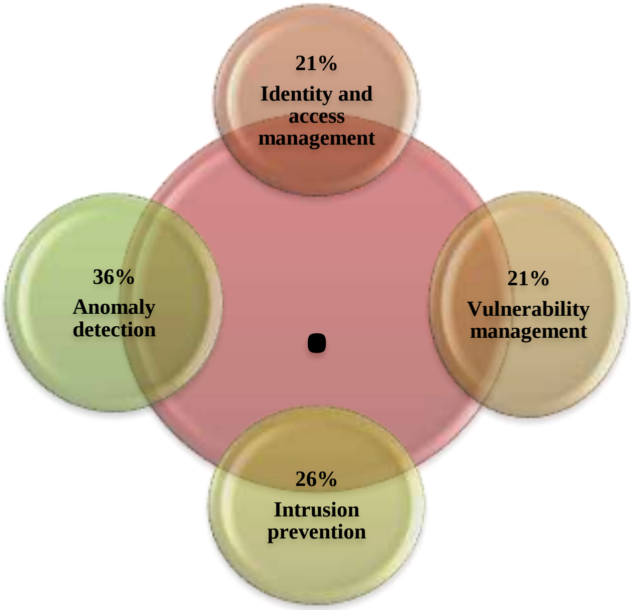

Fig. 4. AI/ML usage in security automation

3.2 Protect

The protection function is critical to mitigate any cybersecurity problems. It involves implementing procedural and technical controls to safeguard against threats from both within and outside. AI technology can contribute to the resilience of systems by enabling a series of preventative measures. These include user authentication, multi-factor authentication, behavioral biometrics, and other physical biometrics. Behavioral biometrics identify unique patterns in observed human behavior, while physical biometrics make use of distinctive physical traits such as fingerprints, patterns of the iris or bio-signals. Intelligent device authentication ensures secure machine-to-machine communication (Manik et al., 2025). Researchers are also exploring approaches for sensor recognition and authentication in domains such as cyber-physical systems and the automotive domain (Md Alamgir Miah, 2025; Nilima et al., 2024). By using AI technology to authenticate users and devices, organizations can fortify their defences, protecting their systems against potential threats and unauthorized access. Fig. 5 shows AI usage in Network security (Ali Linkon et al., 2024; Arpita et al., 2025).

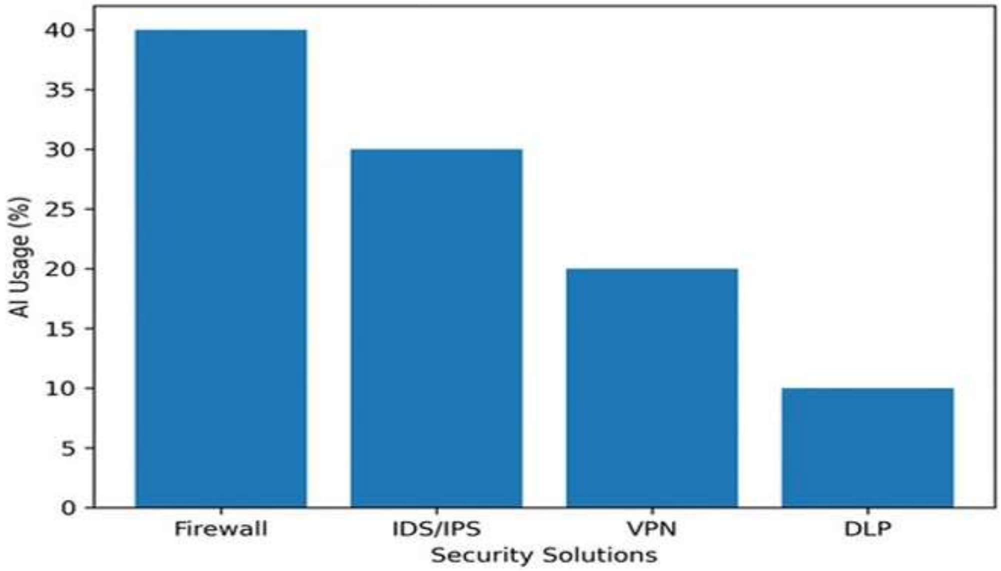

Fig. 5. AI usage in Network security (Siddiqa et al., 2024).

3.3 Detect

The detection function in cybersecurity seeks to find and reduce the disruption caused by cyber threats, through capabilities such as intrusion and anomaly detection, impact assessment and security monitoring (J. Akter et al., 2024). Artificial intelligence (AI) technologies can accelerate detection by monitoring both internal and external information sources and cross-referencing data to identify anomalous activity (Al Mahmud et al., 2025). To detect and mitigate breaches into computer systems, intrusion detection systems (IDS) and intrusion response systems (IRS) are crucial. Techniques such as support vector machines, decision trees, and neural networks enhance their accuracy and efficiency. In malware detection, AI and ML are fundamental because they permit detecting new threats and respond dynamically to emerging trends. Threat hunting has been signature-based historically, but the arrival of AI has changed that dynamic, allowing its predictive powers to facilitate the detection and identification phase (Noor et al., 2024; Sadik et al., 2024). AI systems may ingest huge volumes of endpoint information from a company network and then return comprehensive application profiles that reveal patterns of typical operations. Anomaly detection, in the context of cybersecurity, is critical for identifying a behavior or activity that is unexpected in a system. A widely used AI methodology for anomaly detection is unsupervised machine learning, which consists of algorithms such as density estimation, dimensionality reduction and clustering. Fig. 6 shows anomaly detection.

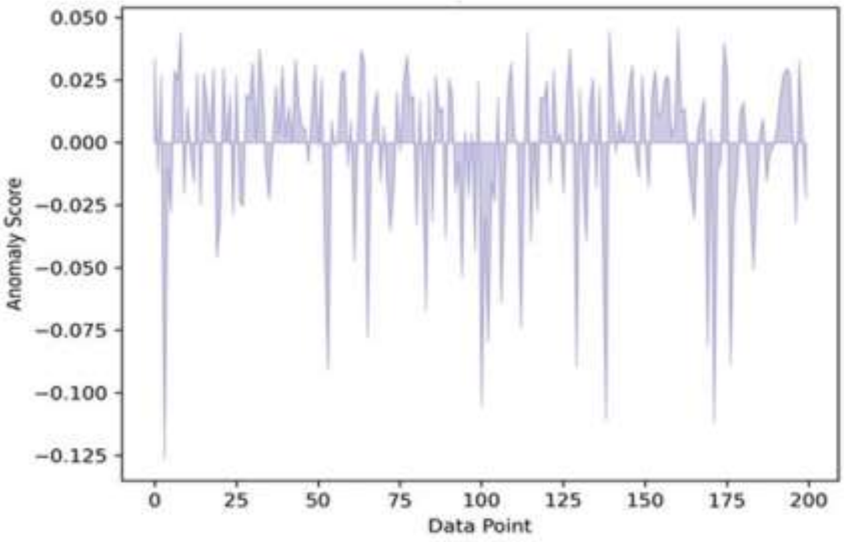

Fig. 6. Anomaly detection (Syed Nazmul Hasan, 2025).

3.4 Respond

The response function is critical for managing and mitigating the impact of cybersecurity events. That involves communication coordination, containment, incident investigation, and proactive planning. AI approaches can process events at a faster rate, enabling security analysts to use their time and energy more efficiently. The reply feature is another important area of research in terms of response planning, automatic spreading of the responsibility, and support systems for collaboratively helping others. How to prepare: Response planning means determining clear protocols, for instance, a contingency plan, that can minimize the extent and impact of an occurrence. An example of automated responsibility allocation is the assignment of incident response tasks in security operation center managers based on staff availability, capability and event type One step further, this can be even a feature of a security operation center manager which assigns incident response activities based on personnel capabilities, as such, you can have an instant incident response generation with a press of a button. Collaboration support systems enable the efficient exchange of data, information, and knowledge among incident response actors. AI approaches are being supported by collaborative analysis platforms to share community knowledge and danger intelligence across sectors. While synchronous systems allow real-time communication for rapid responses, asynchronous systems allow team members to access information at the most convenient time for them. Systems such as Thomas et al. support data processing, real-time communication, and visualization to enable an extensive understanding of threats and the steps taken to handle the threats across multiple analysts.

3.5 Recover

Recovery: In order to ensure that resilience is maintained and can continue to be restored for capabilities affected as a result of successful cyber incidents, the recovery function provides for the ability to recover from such incidents. It aims to minimize the effect, return to normal operations, and learn critical lessons from the experience. Recovery planning involves the preservation and evaluation, and implementation of processes in order to recover assets or systems that have been affected by cybersecurity events. Data recovery involves recovering data from failed servers, while systems recovery involves restoring systems after they go down, both being improved in speed and accuracy through automation made by AI-based recovery planning. However, the literature study did not reveal any significant studies in this area.

Improvement focusing on the evaluation of security incidents to identify areas where the process of recovery planning needs enhancements. AI might automatically analyze incident reports, audit logs and current practices, to identify where improvements can be made and direct future response plans. Analysis and compilation of incident reports meet this need and provide necessary insights for cybersecurity improvement. Artificial intelligence (AI) algorithms could usefully collect, aggregate, extract, visualize and project trends among heterogeneous event data. Meyers and Meneely used natural language processing to build an analytical method that examines vulnerabilities in AU, revealing complex relationships between them through an automated approach.

4. Modelling and analysis

4.1 Case Studies Illustrating the Role of AI in Cyber Security

These real-life instances of the rising use of AI in cybersecurity highlight the growing impact of AI in the industry as they perfect the defensive mechanism, enhance detection of threats, and the management of vulnerabilities.

Symantec's targeted attack analytics (TAA) tool

It uses Artificial Intelligence to sweep through terabytes of data and detect security vulnerabilities. Based on algorithms that mimic how security professionals analyze situations, it identifies targeted attacks with extraordinary accuracy. Knotty was able to prove itself as the most effective tool during the 2018 Dragonfly 2.0 attack, as it was able to step in to save the day and display its proactive threat hunting abilities. The use of AI in tools like TAA is a significant step in the direction of proactive threat detection and incident response. Cybersecurity specialists can use AI to bolster their defenses against and responses to specific attacks, potentially overall enhancing the security of their systems. Fig. 7 shows working Principle of Symantec's TAA tools.

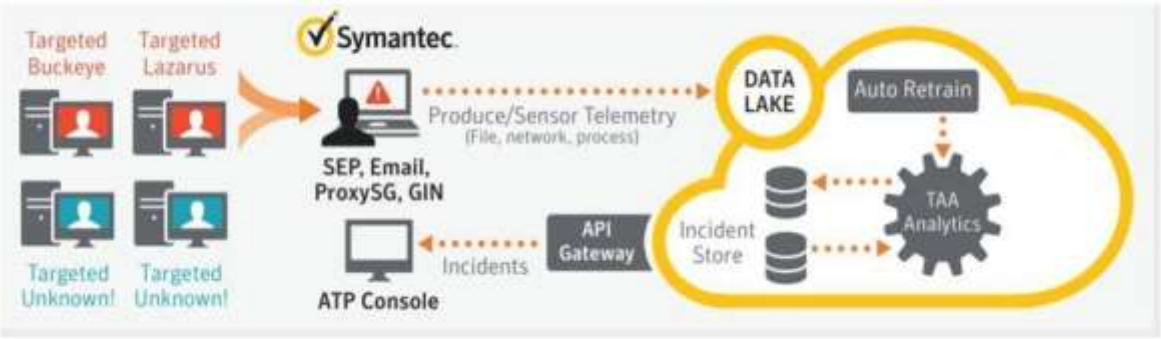

Fig. 7. Working Principle of Symantec's TAA tools

4.1.2. IBM’s QRadar Advisor with Watson

IBM's QRadar Advisor with Watson tool uses cognitive computing to provide an innovative solution for automatically examining potential security issues. This technology gives security analysts the power to appraise threat conditions while minimizing the chance of overlooking crucial threats. This will greatly enhance the accuracy and efficiency in identifying and responding to threats when AI is employed. By analyzing vast amounts of data, the program reliably identifies potential threats. By integrating AI into operations, organizations can not only better their overall security posture but also defend their sensitive assets ahead of time. Fig. 8 shows stages involved in the working of IBM’s QRadar advisor with WATSON .

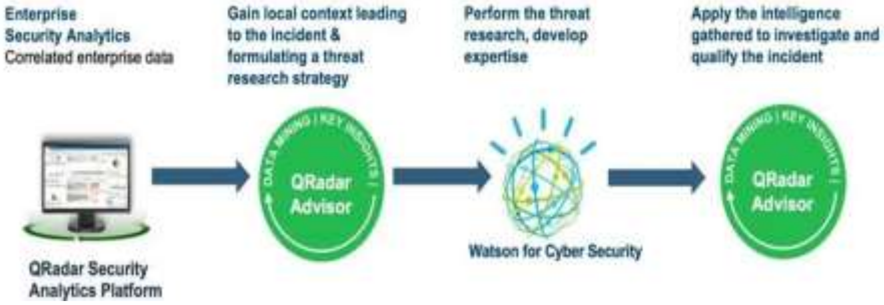
Enterprise
Security Analytics
Correlated enterprise data
Gain local context leading to the incident & formulating a threat research strategy
Perform the threat research, develop expertise
Apply the intelligence gathered to investigate and qualify the incident
DATA MINING | KEY INSIGHTS
QRadar Advisor
Watson for Cyber Security
QRadar Advisor
QRadar Security Analytics Platform

Fig. 8. Stages involved in the working of IBM’s QRadar advisor with WATSON

4.1.3. Sophos’ intercept X

Sophos' Intercept X product employs AI to recognize and prevent malware. It uses deep learning neural networks to differentiate between dangerous and benign files. It can assess the safety and detect potential threats, as well as analyze file features. Its low false-positive rate means fewer harmless files are flagged as harmful. This technology demonstrates the promise that AI holds for cyber security. Fig.9 shows Sophos intercept X.

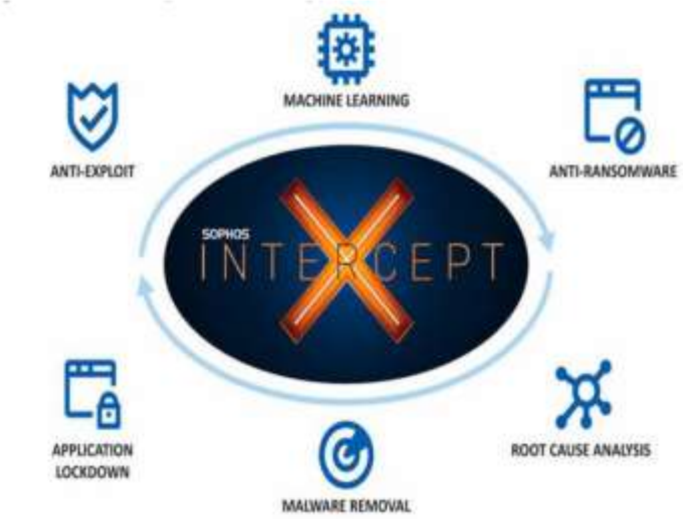

Fig.9. Sophos intercept X

4.`1.4. Deep Locker

A cybersecurity virus known as Deep Locker demonstrates both how AI can be enhanced and how it can also be used to malicious effect. It uses geolocation and face recognition to find its target, which makes it difficult to detect. This story is a reminder of the two sides of AI in cybersecurity, it could enable sophisticated malware to avoid detection, but also enhance defences. However, while generating strong cybersecurity plans, AI must not be abused. Fig. 10 shows Deep locker.

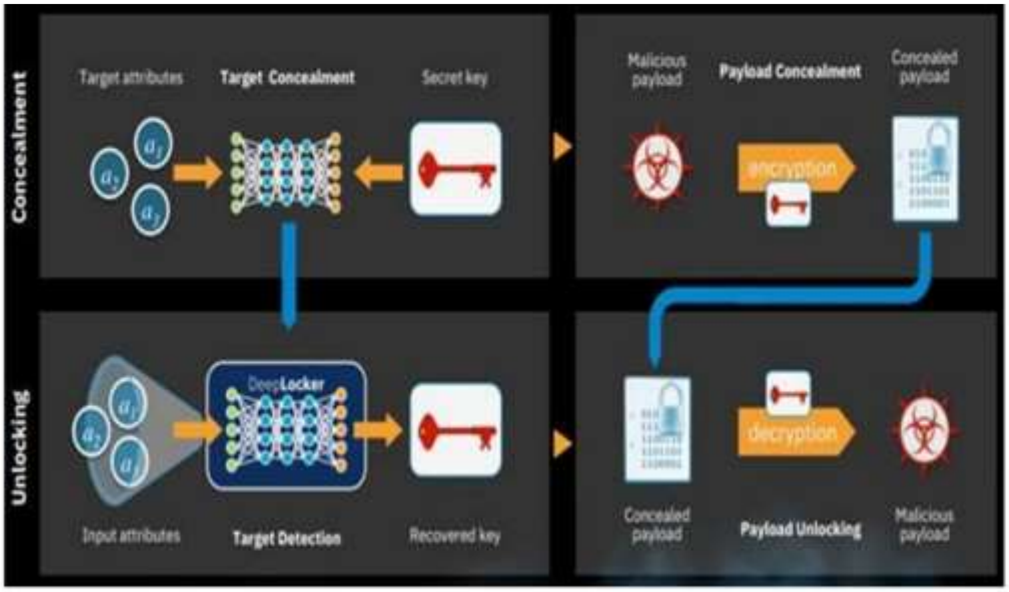

Fig. 10. Deep locker

5. Navigating the challenges and limitations of AI/ML in cybersecurity human adversaries, and AI

A.I. does have some amazing cybersecurity abilities, but it still needs to battle human foes. Human creativity, ingenuity, and flexibility remain a stumbling block, as savvy cybercriminals can evade AI systems. They have tools such as adversarial attacks and data poisoning.

5.1 AI-powered cyber attack

The power of automation and scaling of cyber threats using AI enables cybercriminals to quickly adapt to protective measures, launch attacks at incredible speeds, and exploit weaknesses. Furthermore, it could enable the perpetrators to mimic human behaviour, thus adding legitimacy to phishing attacks. Conventional protection measures may not be enough against very smart and destructive AI-powered malware like Deep Locker. Thus, we have to continue to improve our AI-based defences while making sure human control is in play.

5.2. beyond 5 G technology

Even though beyond 5G innovations generate challenges, such as significant intricacy and extensive network infrastructure needs, they also allow opportunities for CPS in different use cases. Another challenge is the absence of a standardization framework and efficient data management; that is why compatibility and interoperability are matters of concern. Therefore, it requires a large investment.

5.3. Regulatory and legal compliance

Adhering to legal/regulatory requirements for CPS applications includes data protection laws, privacy laws, safety standards, and many more. These specifications can be costly and time-consuming, especially in the healthcare and automobile industries. CPS must also comply with normal legal standards, including privacy and data protection legislation.

6. Results and discussion

Here are some of the most interesting conclusions we have drawn from our extensive research into the present-day trends of using AI and ML in cybersecurity. Such wide implementation of AI and ML in cybersecurity has not gone unnoticed. And the results indicate that a significant percentage of businesses are already implementing AI and ML to bolster their cybersecurity efforts, or plan to do so. They show a growing awareness of how AI and ML could revolutionize cybersecurity and safeguard against attacks online. According to the poll, 35 per cent of companies want to integrate AI and ML into their cybersecurity systems shortly, while 45 per cent of organizations have already done it.

7. Applications of AI and ML in cybersecurity

AI and ML applications in cybersecurity mainly consist of network security, virus detection and intrusion detection. The technology is not without its major barriers to deployment, including a lack of knowledge about its existence and a shortage of qualified staff. Organizations must address these issues to implement AI and ML in cybersecurity effectively (Dutta & Kant, 2020).

8. Future Trends and Predictions in AI/ML and cybersecurity

Artificial intelligence (AI) is radically transforming the cybersecurity landscape in response to the rising digital threats, technical advancements, and the need for adaptive defenses. The AI-Powered Cyber Security market is expected to grow to USD 38.2 billion by the year 2026 (Hutfilter, 2015). That's due to increased data privacy, digitization, and the demand for AI-driven solutions from SMEs and other corporations. As the capabilities of AI technology advance, the tools used for threats and attacks enabled by AI tools become more advanced as well, such as automated phishing attacks and advanced malware. The example of Deep Locker shines a light on why intelligent AI-powered defences are necessary to keep pace with the ever-evolving threat landscape. To counter these new threats, continued investment in state-of-the-art cybersecurity solutions is crucial.

9. Conclusion

It is essential to note that, despite their tremendous promise in the cybersecurity space, AI and ML are not magic bullets. Complexities of Cybersecurity require a comprehensive approach that involves multiple stakeholders such as technologists, lawmakers, legal experts and juxtapositions of technological and traditional solutions. Together we can ensure these technologies are effective and that they are also used ethically and responsibly. In order to gain a better understanding of the ecosystem of AI and ML for cybersecurity, we need to take a holistic perspective and look beyond the technical details.

The key to an effective future in cybersecurity is finding a harmonic balance between the speed and scale of AI and the creativity, intuition and moral judgement of the human mind. By combining the benefits that both approaches offer, this study may be able to detect, mitigate and prevent cyberthreats more holistically.

Openness, accountability, and inclusion should drive the governance of AI in cybersecurity to ensure responsible use. We have to remember that AI is a tool that is supposed to be driven by human values and principles. Everything’s said and done, AI is transforming the cybersecurity domain. With continued research, responsible governance and ethical use, we can harness AI to drive us toward a new dawn as a more secure and safer digital world. While challenges remain, AI offers substantial benefits for cybersecurity, providing a preventive and adaptable approach to protecting our growing connected world.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher’s Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Ahmed, M. K., Bhuiyan, M. M. R., Saimon, A. S. M., Hossain, S., Hossain, S., Manik, M. M. T. G., & Rozario, E. (2025). Harnessing Big Data for Economic Resilience the Role of Data Science in Shaping US Economic Policies and Growth. *Journal of Management*, *2*, 26-34.

[2] Ahmed, M. K., Rahaman, M. M., Khair, F. B., Hossain, S., Hossain, S., Bhuiyan, M. M. R., & Manik, M. M. T. G. (2023). Big Data in Plant Biotechnology: Leveraging Bioinformatics to Discover Novel Anticancer Agents from Flora. *Journal of Medical and Health Studies*, *4*(6), 126-133.

[3] Akter, J., Kamruzzaman, M., Hasan, R., Khatoon, R., Farabi, S. F., & Ullah, M. W. (2024). Artificial Intelligence in American Agriculture: A Comprehensive Review of Spatial Analysis and Precision Farming for Sustainability. 2024 IEEE International Conference on Computing, Applications and Systems (COMPAS),

[4] Akter, T., Samman, A. S. A., Lily, A. H., Rahman, M. S., Prova, N. N. I., & Joy, M. I. K. (2024, 24-28 June 2024). Deep Learning Approaches for Multi Class Leather Texture Defect Classifcation. 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT),

[5] Al Mahmud, M. A., Dhar, S. R., Debnath, A., Hassan, M., & Sharmin, S. (2025). Securing Financial Information in the Digital Age: An Overview of Cybersecurity Threat Evaluation in Banking Systems. *Journal of Ecohumanism*, *4*(2), 1508–1517-1508–1517.

[6] Ali Linkon, A., Rahman Noman, I., Rashedul Islam, M., Chakra Bortty, J., Kumar Bishnu, K., Islam, A., Hasan, R., & Abdullah, M. (2024). Evaluation of Feature Transformation and Machine Learning Models on Early Detection of Diabetes Mellitus. *IEEE Access*, *12*, 165425-165440.

[7] Arpita, H. D., Al Ryan, A., Hossain, M. F., Rahman, M. S., Sajjad, M., & Prova, N. N. I. (2025). Exploring Bengali speech for gender classification: machine learning and deep learning approaches. *Bulletin of Electrical Engineering and Informatics*, *14*(1), 328-337.

[8] Bhuiyan, M. M. R., Noman, I. R., Aziz, M. M., Rahaman, M. M., Islam, M. R., Manik, M. M. T. G., & Das, K. (2025a). Transformation of Plant Breeding Using Data Analytics and Information Technology: Innovations, Applications, and Prospective Directions. *FBE*, *17*(1). https://doi.org/10.31083/fbe27936

[9] Bhuiyan, M. M. R., Noman, I. R., Aziz, M. M., Rahaman, M. M., Islam, M. R., Manik, M. M. T. G., & Das, K. (2025b). Transformation of Plant Breeding Using Data Analytics and Information Technology: Innovations, Applications, and Prospective Directions. *Frontiers in Bioscience-Elite*, *17*(1), 27936.

[10] Biswas, B., Mohammad, N., Prabha, M., Jewel, R. M., Rahman, R., & Ghimire, A. (2024). Advances in Smart Health Care: Applications, Paradigms, Challenges, and Real-World Case Studies. 2024 IEEE International Conference on Computing, Applications and Systems (COMPAS),

[11] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *Ieee Access*, *10*, 93575-93600.

[12] Chowdhury, S. S., Faisal, M. H., Hossain, E., Rahman, Z., Hossin, M. E., & Abdul, M. (2023). Transforming Business Strategies: Management Information Systems, IoT, and Blockchain Technology to Advance the United Nations' Sustainable Development Goals. *American Journal of Computing and Engineering*, *6*(1), 94-110.

[13] Das, N., Hassan, J., Rahman, H., Siddiqa, K. B., Orthi, S. M., Barikdar, C. R., & Miah, M. A. (2023). Leveraging Management information Systems for Agile Project Management in Information Technology: A comparative Analysis of Organizational Success Factors. *Journal of Business and Management Studies*, *5*(3), 161-168.

[14] Debnath, A., Hossan, M. Z., Sharmin, S., Hosain, M. S., Johora, F. T., & Hossain, M. (2024). Analyzing and Forecasting of Real-Time Marketing Campaign Performance and ROI in the US Market. 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA),

[15] Dutta, A., & Kant, S. (2020). An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. Information Systems Security: 16th International Conference, ICISS 2020, Jammu, India, December 16–20, 2020, Proceedings 16,

[16] Ferdousmou, J., Samiun, M., Mohammad, N., Hossan, M. Z., Das, S., Hassan, M., Mozumder, A. Q., & Suha, S. H. (2025). IT Management Strategies for Scaling Artificial Intelligence-Powered Educational Systems in American Schools and Universities. *Journal of Posthumanism*, *5*(2), 470–486-470–486.

[17] Goffer, M. A., Uddin, M. S., kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., Das, N., Chakraborty, P., & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. *Journal of Posthumanism*, *5*(3), 1667–1689. https://doi.org/10.63332/joph.v5i3.965

[18] Hasan, R., Biswas, B., Samiun, M., Saleh, M. A., Prabha, M., Akter, J., Joya, F. H., & Abdullah, M. (2025). Enhancing malware detection with feature selection and scaling techniques using machine learning models. *Scientific Reports*, *15*(1), 9122. https://doi.org/10.1038/s41598-025-93447-x

[19] Hossain, M., Manik, M. M. T. G., Tiwari, A., Ferdousmou, J., Vanu, N., & Debnath, A. (2024). Data Analytics for Improving Employee Retention in the US Technology Sector. 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA),

[20] Hutfilter, A. F. (2015). Estonia: Making the most of human capital. *OECD Economic Department Working Papers*(1214), 0_1.

[21] Imran, M. A. U., Samiun, M., Dhar, S. R., Noor, S. K., & Sozib, H. M. (2024). A Predictive Analysis of Tourism Recovery Using Digital Marketing Metrics. 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA),

[22] Islam, M., Mahmud, F., Khair, F., Hossin, M., Orthi, S., Moniruzzaman, M., & Manik, M. M. T. G. (2025). Advancing Healthcare Management and Patient Outcomes through Business Analytics: A Strategic Approach. *Journal of Management World*, *2025*, 35-45. https://doi.org/10.53935/jomw.v2024i4.866

[23] Islam, M. A., Yeasmin, S., Hosen, A., Vanu, N., Riipa, M. B., Tasnim, A. F., & Nilima, S. I. (2025). Harnessing Predictive Analytics: The Role of Machine Learning in Early Disease Detection and Healthcare Optimization. *Journal of Ecohumanism*, *4*(3), 312-321.

[24] Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, M. I., & Al Mahmud, M. A. (2024). AI Advances: Enhancing Banking Security with Fraud Detection. 2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP),

[25] Kamal, M., Hossin, E., Hossain, S., Khair, F., Hossain, S., Manik, M. M. T. G., & Bhuiyan, M. (2025). Forecasting Sales Trends Using Time Series Analysis: A Comparative Study Of Traditional And Machine Learning Models. *Membrane Technology*, *2025*, 668-682.

[26] Kamruzzaman, M., Bhuyan, M. K., Hasan, R., Farabi, S. F., Nilima, S. I., & Hossain, M. A. (2024). Exploring the Landscape: A Systematic Review of Artificial Intelligence Techniques in Cybersecurity. 2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI),

[27] Kaur, J., Hasan, S. N., Orthi, S. M., Miah, M. A., Goffer, M. A., Barikdar, C. R., & Hassan, J. (2023). Advanced Cyber Threats and Cybersecurity Innovation-Strategic Approaches and Emerging Solutions. *Journal of Computer Science and Technology Studies*, *5*(3), 112-121.

[28] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804.

[29] Khair, F. B., Ahmed, M. K., Hossain, S., Hossain, S., Manik, M. M. T. G., Rahman, R., & Bhuiyan, M. M. R. (2025). Sustainable Economic Growth Through Data Analytics: The Impact of Business Analytics on US Energy Markets and Green Initiatives. *development*, *2*(8), 15-17.

[30] Mahmud, F., Barikdar, C. R., Hassan, J., Goffer, M. A., Das, N., Orthi, S. M., kaur, J., Hasan, S. N., & Hasan, R. (2025). AI-Driven Cybersecurity in IT Project Management: Enhancing Threat Detection and Risk Mitigation. *Journal of Posthumanism*, *5*(4), 23–44. https://doi.org/10.63332/joph.v5i4.974

[31] Manik, M. M. T. G., Rahman, M. M., Bhuiyan, M. M., Islam, M. S., Hossain, S., & Hossain, S. (2025). The Future of Drug Discovery Utilizing Generative AI and Big Data Analytics for Accelerating Pharmaceutical Innovations.

[32] Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: https://www. doi. org/10.56726/IRJMETS32644*, *1*.

[33] Md Alamgir Miah, C. R. B., Habiba Rahman ,Foysal Mahmud ,Jahid Hassan,Shuchona Malek Orthi ,Niropam Das. (2025). Comparative Analysis of Project Management Software: Functionality, Usability, and Integration for Modern Workflows

[34] Article Sidebar. *membrane technology*, *Volume 2025,*(Issue 1). https://doi.org/https://doi.org/10.52710/mt.309

[35] Md Ekrim, H., Jahid, H., Md Asikur Rahman, C., Shafaete, H., Evha, R., Fahmida Binte, K., & Mohammad Abdul, G. (2024). Harnessing Business Analytics in Management Information Systems to Foster Sustainable Economic Growth Through Smart Manufacturing and Industry 4.0. *Educational Administration: Theory and Practice*, *30*(10), 730-739. https://doi.org/10.53555/kuey.v30i10.9643

[36] Md Habibullah Faisal, S. S. C., Md. Sohel Rana, Zahidur Rahman, Emran Hossain and Md Ekrim Hossin. (2022). Integrating artificial intelligence, blockchain, and management information systems for business transformation: A bibliometric-content analysis. *World Journal of Advanced Research and Reviews*, *16*(3), 1181-1188. https://doi.org/https://doi.org/10.30574/wjarr.2022.16.3.1171

[37] Mia Md Tofayel Gonee, M., Evha, R., Sazzat, H., Md Kamal, A., Md Shafiqul, I., Mohammad Muzahidur Rahman, B., & Mohammad, M. (2020). The Role of Big Data in Combatting Antibiotic Resistance Predictive Models for Global Surveillance. *International Journal of Medical Toxicology and Legal Medicine*, *23*(3 and 4). https://ijmtlm.org/index.php/journal/article/view/1321

[38] Miah, M. (2025). Comparative Analysis of Project Management Software: Functionality, Usability, and Integration for Modern Workflows. *Journal of Informatics Education and Research*, *5*. https://doi.org/10.52783/jier.v5i1.2299

[39] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2), 2272358.

[40] Mohammad Abdul, G., Partha, C., Habiba, R., Clinton Ronjon, B., Niropam, D., Sazzat, H., & Md Ekrim, H. (2024). Leveraging Predictive Analytics In Management Information Systems To Enhance Supply Chain Resilience And Mitigate Economic Disruptions. *Educational Administration: Theory and Practice*, *30*(4), 11134-11144. https://doi.org/10.53555/kuey.v30i4.9641

[41] Nilima, S. I., Hossain, M. A., Sharmin, S., Rahman, R., Esa, H., Manik, M. M. T. G., & Hasan, R. (2024). Advancement of Drug Discovery Using Artificial Intelligence and Machine Learning. 2024 IEEE International Conference on Computing, Applications and Systems (COMPAS),

[42] Niropam Das , H. R., Kazi Bushra Siddiqa,Clinton Ronjon Barikdar,Jahid Hassan,Mohammad Muzahidur Rahman Bhuiyan,Foysal Mahmud. (2025). The Strategic Impact of Business Intelligence Tools: A Review of Decision-Making and Ambidexterity. *Membrane Technology*, 542-553. https://doi.org/10.52710/mt.307

[43] Noor, S. K., Imran, M. A. U., Aziz, M. B., Biswas, B., Saha, S., & Hasan, R. (2024). Using Data-Driven Marketing to Improve Customer Retention for US Businesses. 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA),

[44] Prova, N. N. I. (2024a, 28-30 Aug. 2024). Advanced Machine Learning Techniques for Predictive Analysis of Health Insurance. 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI),

[45] Prova, N. N. I. (2024b, 28-30 Aug. 2024). Healthcare Fraud Detection Using Machine Learning. 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI),

[46] Prova, N. N. I. (2024, 3-5 Oct. 2024). Improved Solar Panel Efficiency through Dust Detection Using the InceptionV3 Transfer Learning Model. 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),

[47] Sadik, M. R., Sony, R. I., Prova, N. N. I., Mahanandi, Y., Al Maruf, A., Fahim, S. H., & Islam, M. S. (2024). Computer Vision Based Bangla Sign Language Recognition Using Transfer Learning. 2024 Second International Conference on Data Science and Information System (ICDSIS),

[48] Saimon, A. S. M., Moniruzzaman, M., Islam, M. S., Ahmed, M. K., Rahaman, M. M., Hossain, S., & Manik, M. M. T. G. (2023). Integrating Genomic Selection and Machine Learning: A Data-Driven Approach to Enhance Corn Yield Resilience Under Climate Change. *Journal of Environmental and Agricultural Studies*, *4*(2), 20-27.

[49] Schmitt, J. B., Goldmann, A., Simon, S. T., & Bieber, C. (2023). Conception and interpretation of interdisciplinarity in research practice: Findings from group discussions in the emerging field of digital transformation. *Minerva*, *61*(2), 199-220.

[50] Siddiqa, K. B., Rahman, H., Barikdar, C. R., Orthi, S. M., Miah, M. A., Rahman, R., & Mahmud, F. (2024). AI-Driven Project Management Systems: Enhancing IT Project Efficiency through MIS Integration.

[51] Syed Nazmul Hasan, J. H., Clinton Ronjon Barikdar, Partha Chakraborty, Urmi Haldar, Md Asikur Rahman Chy, Evha Rozario, Niropam Das, Jobanpreet Kaur. (2025). Enhancing Cybersecurity Threat Detection and Response Through Big Data Analytics in Management Information Systems. *Fuel Cells Bulletin*, *2023*(12). https://doi.org/https://doi.org/10.52710/fcb.137

[52] Vacca, J. R. (2013). *Managing information security*. Elsevier.