International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 5589-5598
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

The Influence of Artificial Intelligence on Data System Security

Syed Nazmul Hasan[1], Harleen Kaur[2], Sraboni Clara Mohonta[3], Kazi Bushra Siddiqa[4], Jobanpreet kaur[5*], Urmi Haldar[6], Asikur Rahman Chy[7], Mia Md Tofayel Gonee Manik[8]

[1]College of Technology & Engineering, Westcliff University, Irvine, CA 92614, USA
Email: s.hasan.104@westcliff.edu - **ORCID**: 0009-0008-0977-595X

[2]College of Technology & Engineering, Westcliff University, CA 92614, USA
Email: H.kaur.4088@westcliff.edu - **ORCID**: 0009-0009-7062-0700

[3]Zicklin School of Business, Baruch College, The City University of New York, USA
Email: sraboniclara.m@gmail.com - **ORCID**: 0009-0002-4868-5371

[4]School of Business, International American University, Los Angeles, CA 90010, USA
Email: bushrasiddiqa82@gmail.com - **ORCID**: 0009-0008-0283-9850

[5]College of Technology & Engineering, Westcliff University, CA 92614, USA
*** Corresponding Author Email**: j.kaur.244@westcliff.edu - **ORCID**: 0009-0008-0083-8205

[6]Department of Management, Glasgow Caledonian University, London, UK
Email: UHALDA300@caledonian.ac.uk – **ORCID**: 0009-0000-4040-7583

[7]School of Business, International American University, Los Angeles, CA 90010, USA
Email: mdasikurrahmanchy21@gmail.com -**ORCID**: 0009-0002-6550-7104

[8]College of Business, Westcliff University, Irvine, CA 92614, USA
Email: m.manik.407@westcliff.edu - **ORCID**: 0009-0005-6098-5213

Article Info:

DOI: 10.22399/ijcesen.3476
Received : 11 May 2025
Accepted : 18 July 2025

Keywords

Artificial Intelligence
Cybersecurity
Data System Security
Machine Learning
Intrusion Detection
Anomaly Detection

Abstract:

Data system security has emerged as a top concern for businesses throughout the globe in today's fast-paced digital environment. The increasing sophistication and frequency of cyber-attacks necessitate more sophisticated and flexible forms of defense measures to deal with them. Machine learning, deep learning, and behavioral analytics are all forms of Artificial Intelligence (AI), which has become a revolutionary area of cybersecurity. This paper looks at how AI can enhance the security of a data system in general, and how it can be applied in threat detection, intrusion prevention, malware analysis, and predictive security, in particular. The intertwining of AI technology allows automated responses to potential threats, real-time anomaly detection, and enormous amounts of data processing. This paper gives an informative review of the extent to which AI is transforming the cybersecurity space and enhancing cyber infrastructures through investigating the latest progress and deployment plans.

1. Introduction

Cyber-attacks have become more and more frequent and advanced in the digital, globally connected world, and represent a serious threat to the economic stability, national safety, and the privacy of individuals [1][2]. Cybercriminals find their way through the same flaws and with very sophisticated and continuously developing tactics that require consistent improvements in the utilized protective means. AI has come to play a transformational role in enhancing cybersecurity systems as a response to these rising threats.

AI including its ML and DL approaches appears to provide effective solutions to the multidimensional riddles of cybersecurity. These technologies allow the implementation of smart detection of threats, automated feedback methods, and predictive analytics that remarkably enhance the efficiency of defense actions [3][4]. The current paper discusses how AI can be incorporated in four main areas of cybersecurity like phishing, social engineering, ransomware, and malware. It uses comparative and descriptive analysis to assess AI-based methodologies in these fields, the weaknesses, shortcomings, and fields of expansion.

Cybersecurity is in a critical juncture between rapid innovation and the growth of risks as the rate of digital transformation increases. The interplay of AI and cyber security extends beyond the enhancement of traditional systems by helping increase situational awareness, response to incidents and user training [5] [6]. The paradigm shift is a significant breakthrough in protecting digital infrastructures.

Besides, behavioral threats are becoming subtler in the age of wide-spread internet access. The behavior of the users in different digital platforms can cause major changes in behavior and exposure to threats [7][8]. Conventional tests tend to neglect offline or circumstantial tasks and result in insufficient threat modeling. The spread of multimedia networks and remote access systems have added new vulnerabilities such as unauthorized access, e-fraud, and malware attacks. Therefore, data security in these settings requires systems that can strike the balance between security and access concepts with strong protection mechanisms.

Through these events, encryption has remained a key factor in protecting online information. It is the foundation of data system security giving it confidentiality and integrity of transmission and storage levels [9]. With increasing development of data-driven technologies, encryption continues to play a critical role in deterring unauthorized access and breaches, which supports the overall system of cybersecurity. This paper in conclusion examines the emerging role of AI in cybersecurity of data systems and highlights its presence within the realm of threat detection, behavioral analysis, and encryption.

A. Structure of the Paper

The following is the outline of the paper: Section II offers a overview of security measures for data systems. The function of AI in protecting system data is discussed in Section III. Applications for AI in data system security are discussed in Section IV. A literature overview is provided in Section V, and important results and future prospects are discussed in Section VI.

2. Overview of Data System Security

Data system security refers to the structure of policies, technologies and practices employed to offer security to all digital information and systems against unauthorized access, corruption and theft. Due to increased dependence of organization with connected databases and infrastructure in the cloud, the nature and scope of security threats has been changed rather quickly [10]. The older set of security defenses and in particular those devoted to perimeter defense (i.e. firewalls, intrusion detection systems) are ineffective against the newer and highly mature range of cyber-attacks [11]. Generally, data system security consists of access control, data encryption, anomaly-driven and vulnerability tests. Data systems that work both to protect them against traditional external cyber threats must also develop not only against insider threats, but also against cyber threats caused by the inherent weakness of authentication mechanisms (e.g. passwords), as well as threats caused by malware, phishing and malicious distributed denial-of-service (DDoS) online threats. Also, rapid Internet of Things (IoT) device attachments, programmers that allow remote access to clients all over and general technological convergence have the potential of greatly expanding the attack surface. What this implies is that a modernizing way of data at hand will incorporate the dimension of adaptive and smartness meaning that it comes as a matter of course that an Artificial Intelligence (AI) is introduced to enhance detection, prediction, and response mitigation.

B. Key Concepts and Terminologies

The security of data systems, first of all it is necessary to become familiar with related concepts and terminology. Confidentiality, integrity and availability (the CIA triad) are the three principles of cyber security. It is through confidentiality that sensitive information will only be seen by those people who are supposed to see them. Integrity refers to the fact that data cannot be altered when it is being stored or during the transit process. Availability entails the fact that data and systems are accessible when required by people who are authorized. It also known as authentication (the identification of the person), authorization (granting person access to the specific resources), and encryption (data translation into the form that introduces particular data to other parties) [12]. Firewalls, IDS and IPS are among the many tools used by many organizations to detect and protect networks. It is also important to understand contemporary threats to security like data breach, phishing, malware, ransomware, and zero-day attacks. Similarly, an organization is likely to possess certain awareness regarding how AI is becoming integrated into the security system and the terminology involved therein namely machine learning-based threat identification, or behavioral analysis and automatic response systems, in the context of the cybersecurity environment that has been undergoing alterations over the years.

C. Threat Sources and Classification

Database security issues have multiplied in tandem with the expansion of IT [13]. Data, role, defense system, and external factors are all intimately tied to database

security, and it may scour the literature on the subject to locate them. Thus, it has identified four primary sources of threat: inadequate data protection, malicious users, a weak defense mechanism, and foreign assaults. There are three subsets of data: data that has been tampered with, data that has been exposed, and data that is being observed or gathered. The following types of user exceptions exist: unlawful activity, unauthorized access, and low security awareness. Vulnerability and incorrect identification are further characteristics of a weak defense mechanism. External assaults are the primary cause of database security risks and inflict the most harm. Figure 1 also shows a number of additional categories, such as DDoS assaults, malware, unlawful access, SQL injection, spam, malicious traffic, bypass, and physical attacks.

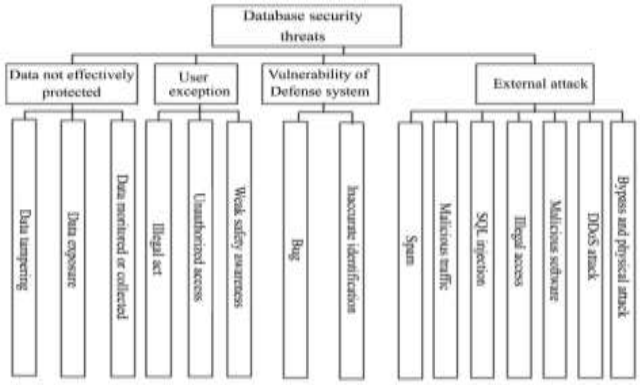

Figure 1. *Sources of database security threats*

D. Traditional Security Architectures

Traditional security approaches to network protection primarily focus on establishing a secure perimeter around an organization's network [14][15]. This model assumes that threats can be effectively blocked at the boundary, allowing trusted users and devices to operate freely within the network

1) Perimeter-Based Security

Perimeter-based security is a foundational principle in traditional network security, emphasizing the creation of a protective boundary that separates an organization's internal network from external threats. This approach is akin to constructing a fortified wall around a castle, where the primary goal is to prevent unauthorized access from outside entities

2) Use of Firewalls and Intrusion Detection Systems

To enforce perimeter security, organizations rely heavily on tools such as firewalls and IDS

- **Firewalls:** The first line of defense is a firewall, which regulates network traffic both inbound and outbound according to preset security rules. It may be software-based, hardware-based, or both.
- **Intrusion Detection Systems (IDS):** Network traffic is monitored by IDS to identify any unusual activities or possible dangers. It can be classified into two main types
  - Network-Based IDS (NIDS)
  - Host-Based IDS (HIDS)

1. Bioenergy refers to electricity and gas that is generated from organic matter,
2. known as biomass. This can be anything from plant and timber to agriculture and food
3. waste and even sewage. Bioenergy includes the production of fuel from organic matter as
4. well. Energy from biomass can be used for electricity, heating, and transportation, and
5. can be replenished anywhere. Around seventy-five percent of the world's renewable
6. energy is composed of biomass energy due to its potential and wide use [7]. Also, it is
7. carbon-neutral, meaning that it adds no net carbon dioxide to the atmosphere. In addition,
8. it reduces the level of trash in the ground by as much as 90 percent by burning solid
9. waste. Biomass fuels, on the other hand, are not completely clean and can also cause
10. deforestation. They are also less efficient than fossil fuels. But proper management and
11. planning of its disadvantages will improve its potential.
12. Bioenergy refers to electricity and gas that is generated from organic matter,
13. known as biomass. This can be anything from plant and timber to agriculture and food
14. waste and even sewage. Bioenergy includes the production of fuel from organic matter as
15. well. Energy from biomass can be used for electricity, heating, and transportation, and
16. can be replenished anywhere. Around seventy-five percent of the world's renewable
17. energy is composed of biomass energy due to its potential and wide use [7]. Also, it is
18. carbon-neutral, meaning that it adds no net carbon dioxide to the atmosphere. In addition,
19. it reduces the level of trash in the ground by as much as 90 percent by burning solid
20. waste. Biomass fuels, on the other hand, are not completely clean and can also cause
21. deforestation. They are also less efficient than fossil fuels. But proper management and
22. planning of its disadvantages will improve its potential.

3. Role of AI in Cybersecurity

AI is changing cybersecurity in Figure 2, helping companies protect their stuff and fight cyberattacks. With AI, security systems can look at tons of info, spot weird stuff, guess when attacks might happen and automatically fight back ASAP. This helps find and stop threats faster and better. Because cyberattacks are getting sneakier, AI is becoming even more important for cybersecurity. It gives us strong ways to fight new dangers and keep important data safe [16].

Figure 2. *AI in Cyber Security*

AI-enabled tools keep learning to make better responses in future incidents depending on what has happened in the past. Including AI solutions, they are able to learn fast of previous behavior and improve the ability to notice anomalies identified in user activity and bad insider threat actors, as well as interfere with or halt damaging action as it is taking place [17]. The fact that AI changes continuously can be considered a tremendous benefit and an aid in building proactive systems. The applications of AI in cybersecurity and its capabilities are going to be of high importance to organizations as the IT environment keeps on changing. Employers that are willing to employ AI have a chance to stay one step ahead of hackers and get improved results in protecting their online assets.

E. Evolution of AI in Cyber Security

In the 21st century, advancements in technology have enabled the exponential expansion of AI evolution. In any case, the present rapid advancements in AI are the result of several decades of study. Alan Turin established the Turing test in the middle of the twentieth century to measure AI, while John McCarthy provided the framework for AI generalizability [18]. These advancements have persisted even if conceptual ideas weren't put into practice until much later in the century. Technology saw potential advancements in data collection and processing technologies as well as an increase in computing power throughout the 1990s. In every other application domain, the idea of machine learning began to gain popularity [19]. The creation of the internet and the exponential rise in processing power demonstrated the full potential of neural network (NN) design and its capacity for intricate analysis. In the late 1900s, the U.S. military emphasized the need of AI in protecting the National Information Infrastructure (NII).

F. AI-Based Threat Detection and Prevention

The complexity and unpredictability of cyberattacks have never been higher. As a result, Artificial Intelligence approaches are now being used in Cybersecurity systems. However, no AI model can be said to be 100 percent accurate. As a result, incorrect predictions occur, necessitating human intervention and response. However, keeping up with the continually growing number is becoming increasingly challenging for human analysts [20][21]. Explainable Artificial Intelligence (XAI) techniques have been developed to address such challenges. There are two aspects to this process. For developing a new model using a training dataset, the first step is to generate the Segment Outlier Score (FOS) information, which is a reliability indicator for AI prediction. The Shapely Additive Explanation (SHAP) model is then used to generate FOS information. It's based on how important each attribute is in AI's training data. The Shapely value extraction formula is as follows equation (1):

$$\phi_i = \sum_{T \subseteq S \subset \frac{F}{j}} \frac{|T|!(|F|-|T|-1)^1}{|F|!} . \left(y(T \cup \{j\}) - y(T)\right) \qquad (1)$$

G. AI and Deep Learning in Cybersecurity

A revolutionary strategy to improve cyber defenses has emerged in his use of AI systems that combine DL with fabricated insights. Cooperative innovation like this uses cutting-edge computer models and computations to fortify defense tools against evolving cyber threats [22][23]. An important part of cybersecurity is the ability to identify complex designs and anomalies in large datasets; profound learning, a branch of machine learning, enables frameworks to learn and adapt from data in a natural way. Neural networks that can detect, categorize, and respond to various cyber threats including malware, phishing attacks, and unauthorized access are part of this system. The goal of this cyber security system that combines deep learning with AI is to not only detect and prevent attacks, but also to simplify incident response and recovery procedures. Automating schedule assignments frees security teams to focus on critical and intricate aspects of cyber defense.

H. Real-World Applications of AI in Cybersecurity

There are various organizations that have successfully deployed AI and ML in their cybersecurity approaches and Figure 3 indicates the applications of AI in cybersecurity.

- **Darktrace:** Darktrace is a company specializing in cybersecurity that involves real-time response and detection of threats using artificial intelligence. Its AI systems analyze the transport of data through networks to identify outliers and normalcy. Darktrace uses the self-learning capabilities to tailor its security tools to the constantly shifting threat landscape by using the distinct network behaviors of each network it protects.
- **Cylance:** Cylance is a company that employs ML to prevent malware. Cylance is based on the properties of files to determine the likelihood of them being malicious as opposed to traditional antivirus that relieve signature databases. This method allows Cylance to identify and thwart new and harmful threats before it can even think of a way to manifest.
- **IBM Watson for Cyber Security:** IBM Watson improves threat intelligence and incident response by integrating AI with conventional security solutions. Through its natural language processing skills, Watson is able to comprehend and correlate intricate threat data from several sources, giving security analysts valuable insights. With this connection, organizations can react to risks with greater speed and efficiency.

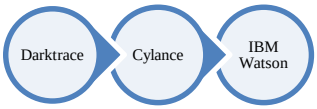

Figure 3. *Applications of AI in cybersecurity*

3. Applications of AI in Data System Security

To determine whether a computer can "think" or if it can do human-level activities, the idea of AI was proposed after the concept of digital computing machines [24]. AI encompasses a wide range of ICT with the overarching goal of creating systems with decision-making capabilities comparable to those of humans [25]. refers to systems that are able to think and learn, and one subtheme is ML, which allows machines to learn from experience by processing vast amounts of data and finding patterns within it. Examples of this include image recognition and Siri.

- A wide range of technologies known as ML enable computers to execute algorithms using data and specific instructions. This gives machines the ability to learn on their own, adapting their algorithms to new situations and situations alone, and even re-coding themselves. An example of this is the ability of voice-activated assistants like Google and Siri to carry out specific tasks [26].
- Deep learning is the next step in machine learning. It simulates the way the human brain processes information by allowing machines to learn and understand data with multiple levels of abstraction, using a large set of data architecture that includes multiple layers.
- Pattern recognition is the backbone of neural networks, which machine learning and deep learning use to learn from observational data and come up with their own solutions. For example, an auto-steering gear system with a fuzzy regulator can choose the best neural network models of the vessel's paths to gain control activity in this way.

İ. Intrusion Detection Systems (IDS)

An IDS detects network intrusion via monitoring of network activities. There are now two primary categories of IDS: host-based and network-based. While host-based HIDSs are made to identify network intrusions in individual hosts, NIDSs are meant to identify intrusions by keeping an eye on various network activity [27]. NIDS monitors packet sniffers' output, and because NIDS can keep an eye on more network targets, it can identify additional assaults that HIDSs could miss since HIDSs are unable to access the packet headers. For instance, NIDS can detect a range of IP-based DoS attacks by keeping an eye on the packet headers travelling across the network [28].

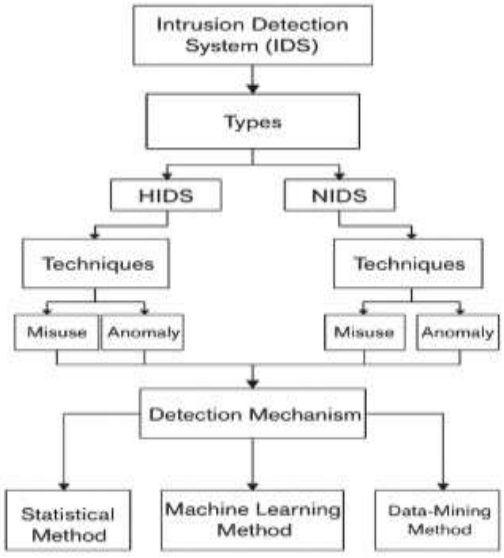

Figure 4. *DS overview*

Furthermore, NIDS depends less on the operating system of the host as a detection source, rather, it is built with specific operating systems to work effectively. HIDS and NIDS have been combined in some hybrid IDSs and used to detect intrusions [29]. Based on the detection mechanism, IDSs are classified into misuse detection (MD) & anomaly detection (AD) systems. Three types of detection mechanisms are used in IDS; these are ML, statistical, and data mining techniques. Figure 4 summarized the IDS

J. Anomaly Detection in Network Traffic

A procedure known as anomaly detection looks for odd patterns in network data. It seeks to locate any security lapses or other problems that could impact the network. For network managers, an anomaly detection system offers a number of benefits [30][31]. It may be used to spot any security risks like malware and hacking attempts. Additionally, it may assist them in locating system malfunctions that can result in downtime. It may also assist them with resource planning and network performance enhancement. Regretfully, network anomaly detection has some limits. Knowing how to differentiate between typical and unusual traffic is a major obstacle. Defining a standard for normalization is not straightforward since the network's behavior might change based on things like the time of day and the user's behavior. The large number of false positives is, however, one of the major drawbacks of anomaly detection solutions. The error of classifying normal traffic as abnormal may be the cause of this. Investigating it may be highly expensive and time-consuming. Furthermore, it is unable to identify assaults that are intended to avoid detection. The security and functionality of computer networks may be preserved with the help of an anomaly detection system. Despite some drawbacks, ML and DL methods may assist increase their accuracy.

K. AI-Driven Security Information and Event Management (SIEM)

The integration of AI into SIEM systems introduces advanced capabilities that enhance threat detection, response, and overall security operations [32]. AI-driven SIEM systems utilize a combination of cutting-edge technologies, each addressing specific challenges [33]

1) *Machine Learning (ML)*

- ML algorithms can discover anomalies by analyzing past data for patterns of typical behavior.
- To identify anomalies that could be signs of danger, both supervised and unsupervised learning models are used.

2) *Natural Language Processing (NLP)*

- NLP aids in parsing unstructured data, such as log entries and threat intelligence reports.
- By interpreting textual data, NLP helps analysts extract actionable insights and identify trends.

3) *Deep Learning (DL)*

- DL models, such as neural networks, are used for complex pattern recognition in large datasets.
- Applications include detecting sophisticated attacks like Advanced Persistent Threats (APTs)

4) *Predictive Analytics*

- Proactive security measures may be implemented with the help of AI's predictive models, which can identify possible weak spots and attack paths.

5) *Automation and Orchestration*

- AI allows for the mechanization of mundane operations, such incident triage and response execution, which lessens the burden on human analysts.

4. Literature Review

An overview and brief summary of the literature on AI and data system security are provided in the next section.

Gorda (2025) a decision-support algorithm designed to assist specialists in conducting efficient and accurate investigations using artificial intelligence techniques. The proposed algorithm incorporates anomaly detection, attacker behavior modeling, and intelligent digital evidence analysis, thereby enhancing the effectiveness of forensic investigations. Furthermore, the developed solution can be further integrated with SIEM systems and digital forensic tools, enabling automated threat correlation and accelerating incident response. The use of AI-driven analytics improves investigation accuracy, reduces the risk of human errors, and optimizes forensic processes in modern cybersecurity environments [34].

Qiu et al. (2024) AI data security, and summarizes the security challenges faced by AI in terms of sensors, operating systems, control systems, and device communications on the basis of combing the AI industry chain; secondly, it combs through the regulatory policies of the world's countries in terms of AI data security; and then it describes the data characteristics of AI in terms of two dimensions, namely, model training and model output; Then, the data security risks of AI are analyzed from both risk types and risk characteristics; finally, measures and suggestions to strengthen AI data security are put forward in response to the risks. The most industrialized nations in the world have identified AI research and development as a top priority in order to boost their competitiveness and ensure their national security in the future [35].

Mohamed (2024) Artificial Intelligence (AI) in countering vulnerabilities that Advanced Persistent Threats (APTs) exploit within cybersecurity frameworks. APTs pose a critical and growing challenge, often outpacing traditional security measures like IDSs and UEBA. By analyzing 30 scholarly articles, delve into various AI-powered approaches, particularly focusing on ML and DL techniques, which have been employed to effectively detect and neutralize risks associated with APTs. The purpose of this article is to provide a critical analysis of AI in cybersecurity by

outlining the current state of the subject, its achievements and failures, and possible future developments [36].

Shetty (2024) AI is already in use and has plenty of room to grow. Keep in mind that there are always going to be obstacles, rules, and security concerns associated with using any technology, including AI. Businesses must carefully monitor the macro issues that may affect the implementation of AI in their operations. The purpose of this research is to provide a high-level summary of the aforementioned obstacles that may affect the adoption of AI; nevertheless, there are a number of tactics and approaches that might assist businesses in overcoming these obstacles. Building and implementing these strategies may take some time, but they will be worthwhile in the end. They will aid in the sustainable deployment of AI and its successful acceptance as a technological enabler [37]

Sankar, Dutta and Karmakar (2024) machine learning approaches for the predictive analysis and assessment of cyber threats. So, various machine learning algorithms provide effective approaches to addressing security issues by using data-driven techniques for cyber threat prediction and assessment, aiming to make an impactful contribution to the research field. Machine learning algorithms are highly effective for solving problems by quickly making decisions, detecting various types of attacks, and predicting the likelihood of cyber-attacks on the network. In addition, the issues of machine learning adoption in cyber security are examined, such as privacy of data, comprehending the operation of the model, and defending against cyber-attacks. Machine learning approach enhances security protection and prevention by detecting cyber threats early and automatically responding to them [38].

Barton et al. (2024) developments in AI for cybersecurity, opportunities for improvement, and challenges to further AI's use in this field. Cybersecurity technologies built on AI have become more useful to security professionals as the field has seen rapid innovation and automation in recent years. Data privacy, security holes, and AI biases are all issues with the data used to train AI, which raises worries about its application. The problem of trust between computers and people is another issue. An organized assessment of AI developments in cybersecurity and worries about AI adoption is the goal of this research. It does this by sifting through scholarly publications on AI in cybersecurity published between 2022 and 2024 and offering suggestions for new research projects [39].

Priya et al. (2023) has been said that "data is money" and that such information is vital to the prosperity of any enterprise. There must be strict measures in place to guarantee the security of stored data for this reason. True regardless of a company's industry. Because of the administrative interdependence of data security and integrity for enforcement purposes, a solution is required for data management that can certify both at the same time. This article makes an effort to catalogue the many areas where AI tools contribute to effective data integrity and security, while simultaneously focusing on the gaps and missing pieces that need to be filled in order to remove the obstacles to AI tool use [40].

Table 1 provides an overview of the literature on AI on Data System Security, methods, key findings, challenges, and future directions.

TABLE I. SUMMARY OF RECENT STUDIES ON ARTIFICIAL INTELLIGENCE APPLICATIONS IN CYBERSECURITY AND DATA SECURITY

Author	Study On	Approach	Key Findings	Challenges	Future Directions
Gorda et al. (2025)	AI-based decision support in digital forensic investigations	Anomaly detection, attacker modeling, AI-driven evidence analysis	Improves investigation accuracy and response speed by integrating AI with SIEM and forensic tools	Integration with existing forensic systems; trust in automated evidence analysis	Enhanced automation, real-time threat correlation, integration with broader cybersecurity ecosystems
Qiu et al. (2024)	AI data security in global contexts	Regulatory analysis, risk assessment, and industry chain review	Identifies risks at sensor, OS, control system, and communication levels; summarizes global policy landscape	Varying regulations, high complexity in securing AI models	Develop standardized global data security frameworks for AI
Mohamed et al. (2024)	Use of AI to combat Advanced Persistent Threats (APTs)	Literature review on ML/DL for APT detection	AI methods outperform traditional IDS/UEBA in APT detection	Evasion techniques by APTs; limited generalizability of models	More robust and adaptive ML models; real-time APT threat intelligence sharing

Shetty et al. (2024)	Barriers and enablers of AI adoption in businesses	Review of AI implementation issues and solution strategies	Lists macro-level factors affecting AI adoption; proposes strategic solutions	Regulatory, technological, and cultural adoption barriers	Build long-term adoption strategies with scalability and resilience
Karmakar et al. (2024)	ML-based cyber threat prediction and assessment	Supervised ML models for detection and prediction of cyber threats	ML improves early threat detection and decision-making	Model transparency, data privacy, and adversarial attacks	Enhancing explainability and robustness of ML in cybersecurity
Barton et al. (2024)	Review of AI advancement and inhibitors in cybersecurity	Systematic literature review of 2022–2024 articles	AI improves automation and efficiency in cybersecurity tools	AI bias, data privacy, trust issues, implementation limitations	Foster explainable AI, address trust gaps, improve data governance in AI systems
Priya et al. (2023)	Role of AI in ensuring data integrity and security across sectors	Sector-wide review of AI applications in data management	AI helps enforce data integrity and security standards	Data silos, unaddressed vulnerabilities, insufficient AI integration	Address integration gaps and develop AI tools tailored for cross-sector data security

6. Conclusion and future work

The cybersecurity environment is being transformed by AI, which provides automated solutions that are intelligent, dynamic, and able to withstand more complex cyber assaults. Through the integration of AI-driven technologies like ML, DL, and behavioral analytics, security systems can proactively detect anomalies, predict potential attacks, and respond in real-time. This paper has highlighted the application of AI in critical areas like malware detection, phishing, social engineering, intrusion detection systems, and AI-augmented SIEMs. Although AI can enhance reaction time and accuracy in detecting threats, some of its issues, such as incomprehensible models, false positive detection, and data privacy ethical concerns are emerging. Nevertheless, the synergy between cybersecurity and AI outlines a radical direction of resilient and adaptive safety and security of data systems. AI is one of the most effective tools in this effort to protect digital structure, guarantee information secrecy, and enhance organizational protection. Nonetheless, AI models currently lack transparency, and there is complexity in comprehending decision-making processes. Moreover, excessive focus on AI may cause complacency and vulnerability to possible failures in case systems are not frequently checked and upgraded.

Future research in AI-based cybersecurity must aim at developing easier to understand and explain AI models in an attempt to make automated security decisions more transparent and trustworthy. False positives harmonically decreased, and the greater accuracies of anomaly detection systems remain an important objective. In addition, a study in how AI can be combined with novel technology such as federated learning, blockchain, and quantum computing could result in decentralized systems of data security that are more secure and convenient to adopt. International collaboration is also necessary to solve regulatory and ethical challenges, particularly regulated in relation to AI access sensitive information. Moreover, the AI models should be drawn to be resistant to adversaries' attacks and learn and adjust to varying riverbeds of threats. Development of standardized frameworks and international regulatory guidelines on adoption of AI in cybersecurity will create a solid, scalable, and morally acceptable implementation in future.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] K. Arockiasamy, (2023). The Role of Artificial

Intelligence in Cyber Security, in *AI Tools for Protecting and Preventing Sophisticated Cyber Attacks*, vol. 8(10), 1–24. doi: 10.4018/978-1-6684-7110-4.ch001.

[2] S. S. S. Neeli, (2022). Critical Cybersecurity Strategies for Database Protection Against Cyber Attacks, *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1(1). 2102–2106, doi: 10.51219/JAIMLD/sethu-sesha-synam-neeli/461.

[3] S. Okdem and S. Okdem, (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study, *Appl. Sci.*, vol. 14(22), doi: 10.3390/app142210487.

[4] N. Malali and S. R. P. Madugula, (2025). Robustness and Adversarial Resilience of Actuarial AI/ML Models in the Face of Evolving Threats, *Int. J. Innov. Sci. Res. Technol.*, vol. 10(3), 910–916, doi: 10.38124/ijisrt/25mar1287.

[5] M. Mikic and J. Malala, (2021). The impact of artificial intelligence on the future of work, in *The Home in the Digital Age, Milton Park, Abingdon, Oxon ; New York : Routledge, Series: Routledge advances in sociology: Routledge*, 143–159. doi: 10.4324/9781003080114-8.

[6] P. Piyush, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, (2024). Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis, *J. Intell. Syst. Internet Things*, vol. 24(2), 195–207, 2024, doi: 10.54216/JISIoT.120215.

[7] M. Zulfadhilah, (2017). The Importance Of Securing Digital Data, *Proc. 2nd Sari Mulia Int. Conf. Heal. Sci. 2017 (SMICHS 2017)*, vol. 6, 431–435, doi: 10.2991/smichs-17.2017.53.

[8] V. Thangaraju, (2025). Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques, *Int. Res. J. Innov. Eng. Technol.*, vol. 9(3), 205–212, 2025, doi: 10.47001/IRJIET/2025.903027.

[9] P. Goyal, P. Sharma, M. Sharma, and A. Pareek, (2023). The Importance of Data Encryption in Data Security, *J. Nonlinear Anal. Optim.*, vol. 13(1), 1–11, doi: 10.36893/jnao.2022.v13i02.001-011.

[10] W. Febriyani, T. F. Kusumasari, and M. Lubis, (2023). Data Security: A Systematic Literature Review and Critical Analysis, in *2023 International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS)*, IEEE, 1–6. doi: 10.1109/ICADEIS58666.2023.10270832.

[11] A. Mishra, (2025). AI-Powered Cybersecurity Framework for Secure Data Transmission in Iot Network, *Int. J. Adv. Eng. Manag.*, vol. 7(3), 05–13, doi: 10.35629/5252-07030513.

[12] R. A. Teimoor, (2021). A Review of Database Security Concepts, Risks, and Problems, *UHD J. Sci. Technol.*, vol. 5(2), 38–46, doi: 10.21928/uhdjst.v5n2y2021.pp38-46.

[13] Y. Wang, J. Xi, and T. Cheng, (2021). The Overview of Database Security Threats' Solutions: Traditional and Machine Learning, *J. Inf. Secur.*, vol. 12(1), 34–55, doi: 10.4236/jis.2021.121002.

[14] A. A. Wells, K. Ajeigbe, and M. Stern, (2025). Security Trends in Networking : From Traditional Approaches to Zero Trust Architectures.

[15] V. Kolluri, (2020). A Detailed Analysis of AI as a Double-Edged Sword: AI-Enhanced Cyber Threats Understanding and Mitigation, *Int. J. Creat. Res. Thoughts*, vol. 8(7), 2320–2882.

[16] Adish K and Venkatesh, (2022). A Review Paper on Cyber Security, *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 11(10), 528–531, doi: 10.48175/IJARSCT-2920.

[17] S. Chatterjee, (2021). Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry, *Int. J. Multidiscip. Res.*, vol. 3(4), 1–10, doi: 10.36948/ijfmr.2021.v03i04.34396.

[18] A. K. Polinati, (2025). AI-Powered Anomaly Detection in Cybersecurity: Leveraging Deep Learning for Intrusion Prevention," *Int. J. Commun. Networks Inf. Secur.*, vol. 17(3), 301–323.

[19] A. Mishra, (2025). AI-Powered Cyber Threat Intelligence System for Predicting and Preventing Cyber Attacks, *Int. J. Adv. Eng. Manag.*, vol. 7(2), 873–892, doi: 10.35629/5252-0702873892.

[20] K. S. Kandala, D. V. Sai, N. Saketh, I. Neelima, and B. Alekhya, (2022). Artificial Intelligence Techniques for Prevention of Cyber Attacks and Detection of Security Threats, *Int. J. Eng. Res. Appl. www.ijera.com*, vol. 12, 37–44, doi: 10.9790/9622-1206053744.

[21] S. S. S. Neeli, (2025). A Hands-On Guide to Data Integrity and Privacy for Database Administrators, *Int. J. Sci. Res. Eng. Manag.*, vol. 9(1), 1–6, doi: 10.55041/IJSREM16443.

[22] I. Hamid and M. M. H. Rahman, (2025). AI, machine learning and deep learning in cyber risk management, *Discov. Sustain.*, vol. 6(1), doi: 10.1007/s43621-025-01012-3.

[23] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, (2024). Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality, in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, IEEE, 1–6. doi: 10.1109/ACET61898.2024.10730334.

[24] M. J. Correia and F. Matos, (2021). The impact of artificial intelligence on innovation management: A literature review, *Proc. Eur. Conf. Innov. Entrep. ECIE*, 222–230, doi: 10.34190/EIE.21.225.

[25] H. Kali, (2023). The Future of HR Cybersecurity: AI-Enabled Anomaly Detection In Workday, *Int. J. Recent Technol. Sci. Manag.*, vol. 8(6).

[26] D. D. Rao, S. Madasu, S. R. Gunturu, C. D'Britto, and J. Lopes, (2024). Cybersecurity Threat Detection Using Machine Learning in Cloud-Based Environments: A Comprehensive Study, *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 12(1), 285–290.

[27] S. Singamsetty, (2019). Fuzzy-Optimized Lightweight Cyber-Attack Detection for Secure Edge-Based IoT, *J. Crit. Rev.*, vol. 6(7), 1028–1033, doi: 10.53555/jcr.v6:i7.13156.

[28] M. Aljanabi, M. A. Ismail, R. A. Hasan, and J. Sulaiman, (2021). Intrusion Detection: A Review, *Mesopotamian J. CyberSecurity*, 1–4, doi: 10.58496/MJCS/2021/001.

[29] V. Prajapati, (2025). Enhancing Threat Intelligence and

Cyber Defense through Big Data Analytics: A Review Study, *J. Glob. Res. Math. Arch.*, vol. 12(4), 1–6, doi: https://zenodo.org/records/15223174.

[30] S. Ness, V. Eswarakrishnan, H. Sridharan, V. Shinde, N. V. P. Janapareddy, and V. Dhanawat, (2025). Anomaly Detection in Network Traffic using Advanced Machine Learning Techniques, *IEEE Access*, vol. 10(2), 1063–1067, doi: 10.1109/ACCESS.2025.3526988.

[31] N. Prajapati, (2025). Federated Learning for Privacy-Preserving Cybersecurity : A Review on Secure Threat Detection, *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5(4), 520–528, doi: 10.48175/IJARSCT-25168.

[32] S. B. Shah, (2025). Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure, *Dep. Oper. Bus. Anal. Inf. Syst. (OBAIS*, vol. 2(2), 1–7, doi: 10.5281/zenodo.14955016.

[33] O. Timilehin, (2022). AI in Security Information and Event Management: Transforming User Experience and Decision-Making AI in Security Information and Event Management: Transforming User Experience and Decision-Making Author; Oladoja Timilehin.

[34] M. Gorda, (2025). On the Use of Artificial Intelligence in Cybersecurity Incident Investigations, in *2025 International Russian Smart Industry Conference (SmartIndustryCon)*, 747–752. doi: 10.1109/SmartIndustryCon65166.2025.10986177.

[35] B. Qiu, D. Liu, S. Cao, C. Mu, S. Yan, and Y. Liu, (2024). Risk Analysis and Protection Suggestions for Artificial Intelligence Data Security, in *2024 IEEE 9th International Conference on Data Science in Cyberspace (DSC)*, 392–398. doi: 10.1109/DSC63484.2024.00059.

[36] N. Mohamed, (2024). Artificial Intelligence in Cybersecurity: A Review of Solutions for APT-Exploited Vulnerabilities, in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–7. doi: 10.1109/ICCCNT61001.2024.10724084.

[37] P. Shetty, (2024). AI and Security, From an Information Security and Risk Manager Standpoint, *IEEE Access*, vol. 12, 77468–77474, doi: 10.1109/ACCESS.2024.3408144.

[38] S. Sankar, R. Dutta, and S. Karmakar, (2024). Cyber Threat Prediction and Assessment with Machine Learning Approaches, in *2024 IEEE 21st India Council International Conference (INDICON)*, 1–6. doi: 10.1109/INDICON63790.2024.10958346.

[39] R. Barton, P. W. C. Prasad, I. Seher, and A. Elchouemi, (2024). Artificial Intelligence (AI) in Cybersecurity and Inhibitors to AI Adoption, in *2024 International Conference on Intelligent Education and Intelligent Research (IEIR)*, 1–10. doi: 10.1109/IEIR62538.2024.10959777.

[40] V. L. Priya, A. A, A. Chahar, and A. A, (2023). Artificial Intelligence as a Tool for Enhanced Data Integrity and Data Security, in *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, IEEE, 781–785. doi: 10.1109/AISC56616.2023.10085250.