World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Enhancing cybersecurity audits with AI an automated approach to risk management

Suneel Kumar Mogali *

Perficient, Inc.

World Journal of Advanced Research and Reviews, 2023, 17(02), 954-963

Publication history: Received on 08 January 2023; revised on 23 February 2023; accepted on 25 February 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.17.2.0291

Abstract

Integrating AI into cybersecurity practices is essential for improving and speeding up auditing processes in today's fast-paced digital world. Examining the many effects of AI automation on cybersecurity audits, this study delves into the topic. Based on the latest findings, AI has the potential to revolutionize cybersecurity by identifying potential threats early on, resolving difficulties swiftly, and equipping enterprises to face emerging cyber threats. AI-driven cybersecurity audits analyse large amounts of data in real-time using sophisticated computer programs, looking for unusual or suspicious patterns that could indicate a vulnerability. With the help of AI's insightful forecasts, businesses can head off issues before they even start. Together, AI and cybersecurity are a hot topic, and we cover how AI tools improve security and simplify audits. With the use of specialized AI algorithms, such as threat-spotting systems, enterprises can detect, halt, and resolve cyber threats with more intelligence. To ensure thoroughness and accuracy, this article also delves into how AI enhances audits.

Keywords: Cybersecurity; Artificial intelligence; Risk Management; AI-Driven Cybersecurity; Cyber Threat Intelligence

1. Introduction

Cybersecurity is a major issue for governments, corporations, and individuals in today's technologically advanced world. While developments in AI systems present exciting new possibilities for risk assessment and mitigation, they also bring with them brand-new obstacles. As a result, studying the relationship between AI and cybersecurity is becoming more important both today and in the future [1]. Becoming a cybersecurity expert is within your reach with the help of the specialized courses offered by the top BTech AI and Data Science schools in Tamil Nadu. These programs combine classroom instruction with practical experience.

Protecting digital systems is the focus of cybersecurity, whereas artificial intelligence (AI) is a subfield of computer science concerned with creating machines capable of tasks normally requiring human intelligence. By combining their respective strengths, these two areas can shed light on how to best train and educate AI systems to detect cyber dangers using real-world cyber security data [2]. Cyber security systems now incorporate AI to automate threat detection and response processes or to forecast network breaches based on previous patterns. This helps to design security infrastructures that can adapt to new threats as they emerge. KAHE provides specialized programs in data science and artificial intelligence and is considered one of the best BTech AI institutes in Coimbatore [3].

1.1. Areas where AI is significantly impacting cyber security

By delivering potent tools for identifying and avoiding cyber threats, protecting sensitive data, and improving overall security, artificial intelligence (AI) is transforming the cybersecurity industry.

* Corresponding author: Suneel Kumar Mogali

- **Detect and thwart cyber-attacks:** In order to find and stop new kinds of attacks on your digital assets, it can sift through mountains of data, find dangers, and create algorithms.
- **Safeguard data:** It makes it harder for unethical hackers to access your company's sensitive data by encrypting it, monitoring data access, and identifying unauthorized users.

Among the top AI schools in Tamil Nadu, KAHE provides courses in data science, machine learning, and artificial intelligence.

1.2. Advantages of AI in Cybersecurity:

A wide range of useful and advantageous outcomes can be achieved by combining AI with cybersecurity technologies.

- **Monitor network traffic:** It protects sensitive information from cyber dangers that human specialists miss and efficiently monitors data exchanges between your firm and stakeholders.
- **Detect unknown threats:** It can detect and prevent unforeseen cyberattacks on your digital assets, which are difficult for cybersecurity experts to detect and may do significant harm before they are discovered.
- **Mitigating threats:** As data flows continuously into and out of your organization's network, it can efficiently identify and block malicious data.
- **Continual learning:** AI systems are able to proactively respond to any security threats, find patterns, and organize them through their ongoing learning features, which boost their capabilities.
  When it comes to BTech AI schools in Coimbatore, KAHE is among the best options for students interested in data science and artificial intelligence.
- **Automating repetitive processes:** By incorporating AI technologies, you may automate fundamental security measures, reducing the likelihood of network vulnerability caused by human error or exhaustion.
- **Comprehensive security:** With AI, your digital systems are completely protected from any and all dangers. It can handle numerous threats at once and respond quickly and appropriately to each one.
- **Enhanced endpoint protection:** An essential part of device security, it solves problems faced by big companies with many networked devices and offers strong defense against malware and ransomware using recognized signatures.
- **Efficient data handling:** Additionally, AI systems efficiently handle the massive amounts of data that are transmitted across your company's networks, guaranteeing thorough scanning and analysis that goes beyond what humans are capable of.
  KAHE is a top AI school in Tamil Nadu, India, with courses that will teach you all you need to know about AI, ML, and data science.
- **Risk prediction:** By processing inventories and evaluating IT assets, AI systems may help your firm anticipate and prepare for cyber attacks, as well as transfer resources to susceptible areas as needed.
- **Strengthen authentication:** Protecting sensitive data such as login credentials, credit card details, and other financial information is a top priority for commercial websites, and AI adds an extra degree of protection in this regard.

1.3. Challenges associated with integrating AI and cyber security systems:

Nevertheless, this procedure is not without its difficulties, such as the possibility of unexpected false positives or the risk of relying too much on outdated data when confronted with novel threats. Cybercriminals may employ hostile AI systems to find loopholes in digital defenses that algorithms haven't been programmed to detect. Despite these obstacles, AI progress can improve cybersecurity standards by lowering the threshold for undetected security threats through improved anomaly detection or predictive skills [4]. When you want to get a better grasp of data science and artificial intelligence, KAHE is a great option among the top BTech AI schools in Coimbatore.

Protecting digital assets and enhancing the company's reputation among consumers necessitates ethical standards when using AI for cybersecurity challenges. When dealing with ever-changing cyber dangers, it's important to invest in high-quality, diverse data sources to provide dependable findings. In cybersecurity initiatives, AI can be utilized to enhance human capabilities.

2. Literature review

Constant change and ever-increasing complexity define the cyber threat landscape. Cybercrime has evolved into a substantial industry that tests the resilience of even the most robust defenses, thanks to its increasing regularity and sophistication in recent years [5]. Modern cyber threats are characterized by their ingenuity and scale, as shown in high-profile occurrences like the SolarWinds and Colonial Pipeline attacks. The techniques employed by cybercriminals and the weaknesses of existing cybersecurity solutions can be better understood from these occurrences [6]. These two major cyberattacks show the variety and breadth of cybersecurity threats. Lessons learnt on vulnerabilities and the need for improvements to cybersecurity practices are the primary focus of the analysis.For a better grasp of the processes and consequences of complex cybersecurity breaches, two notable case studies are the SolarWinds and Colonial Pipeline hacks. In 2020, the Orion platform's software updates were the subject of the SolarWinds hack, a supply chain assault that was thought to have been carried out by a nation-state actor. Trust between software vendors and their customers was a weak spot that this attack took advantage of, compromising thousands of businesses around the world, including some branches of the United States government. Stronger software update checks and tighter supply chain security measures are necessary in light of the incident. On the other hand, a cybercrime gang launched a ransomware attack on Colonial Pipeline in May 2021 [7]. By taking advantage of security holes, the pipeline network's information technology systems were the intended targets. Damage to the fuel delivery system in the East Coast of the United States was one of the many operational and financial consequences of the attack. The tragedy highlighted the need for better ransomware defenses and the susceptibility of vital infrastructure to cyber threats. The significance of bolstering cybersecurity measures in several domains, such as critical infrastructure protection and the supply chain, is underscored by both instances taken together [8].

To combat the complex risks that contemporary enterprises encounter, AI and ML are leading the charge to reshape cybersecurity strategy. When these technologies are incorporated into cybersecurity frameworks, security systems are able to improve their capabilities in multiple important ways [10]. One area where AI and ML really shine is in spotting possible security risks at an early stage. These smart systems can detect security breaches by constantly monitoring massive volumes of network data in real time for irregularities and patterns. Artificial intelligence (AI) is a potent weapon against zero-day assaults and advanced persistent threats (APNs), which often evade standard security controls because they learn to detect new and changing dangers, in contrast to traditional security measures[11]. Artificial intelligence and machine learning not only improve cybersecurity detection, but also analysis. They are able to discover hidden dangers by sorting through and correlating different data points throughout an organization's digital infrastructure, such as server logs and network traffic. Machine learning models are able to analyze this data more thoroughly and faster than human analysts could by using complicated algorithms. By delving into the context and level of sophistication of the attack vectors, businesses can improve their strategic response [12]. Security incident response may be further automated with the use of AI and ML. Isolating impacted systems, blocking suspect IP addresses, or terminating harmful processes are all examples of predetermined actions that AI-driven systems can implement upon threat detection. This kind of automatic reaction is vital for reducing the impact of threats like ransomware, which propagate quickly throughout networks. Adaptive security postures are also made possible by AI and ML [13]. Machine learning models can improve their forecasting power by learning from each attack attempt. These systems can anticipate and avert future assaults by learning the TTPs of the attackers. AI can also be useful for managing security policies by suggesting changes to IDSs, firewalls, and other security measures in response to changing threat scenarios. Security solutions backed by AI may also grow with the company as its digital infrastructure does. Machine learning and artificial intelligence systems can increase their monitoring capabilities with no corresponding increase in human personnel or expenditures, even if the amount of data and endpoints increases. As a company expands and its threat surface widens, these scalable security solutions will keep working [14].

2.1. Ethical Considerations and Policy Implications of AI in Cybersecurity

Integrating ML and AI into cybersecurity improves capabilities but also requires careful analysis of technical, ethical, and regulatory issues [15, 16]. The ethical issues surrounding cybersecurity and the technical advances made possible by AI and ML are both brought together in this consolidated and expanded discussion. Ethical questions like privacy, permission, and openness are at the forefront of discussions about using AI in cybersecurity. The effective detection of risks by AI systems frequently necessitates access to massive volumes of personal data, which can limit privacy rights. Training AI models on data sets that do not accurately reflect the population at large might lead to biases in their decisions, which in turn can pose ethical problems. Data reduction, anonymization methods, and the establishment of transparent permission mechanisms are critical initiatives to address these concerns [17]. The General Data Protection Regulation (GDPR) and other strong legal frameworks show how regulations can assist strike a balance between security needs and privacy rights [18]. For artificial intelligence (AI) applications in cybersecurity to adhere to stringent norms of data protection and ethical responsibility, such frameworks impose stringent rules on data processing techniques.

3. Artificial intelligence as a tool for cybersecurity audits

Artificial intelligence (AI) in cybersecurity audits collects data on cyber threats and events from many sources, processes it, and then presents the results in a way that security experts can understand and utilize for further investigation, response, and reporting. Through the use of AI, the security team may automate the reaction to cyberattacks that fulfill specific criteria, allowing them to isolate the affected assets. To take it a step further, generative AI can identify patterns in data and use them to generate new content, such as text, graphics, and natural language.

3.1. AI for cybersecurity audits

Cybersecurity audit: This determines how well digital data is protected against various dangers such as cyber-attacks, flaws, competing software, and phishing attempts.

A "information security audit" is a term that appears frequently online. Cybersecurity auditing is part of the larger field of surveillance, which this phrase encompasses. The goal of an information security audit is to detect and prevent security breaches, such as data leaks caused by social engineering on the part of workers or successful cyberattacks on an organization's IT infrastructure.

3.2. Types of Cybersecurity Audits:

3.2.1. Internal audit

Using charters and other corporate papers, controls the inner workings of the business. Finding potential weak spots in the company system that could lead to the disclosure of critical information is the main goal of the scan.

It is acceptable to form a commission of qualified employees or to bring in outside specialists to carry out an internal audit; the legislation does not dictate anyone's role in this process. Experts in the company's security and infrastructure management divisions are usually tasked with the assignment.Organizational needs and objectives dictate the regularity of internal audits. At least twice or thrice a year, with a well-thought-out strategy and a team of experts on hand, you should have the operation done. On a daily basis, you can also verify that web services, network infrastructure, and sensitive data are secure.

3.2.2. External audit

There is no difference between internal and external audits in terms of their aims and purposes. The key distinction is that in an external audit, third-party specialists are granted access to the company's internal databases. This form of verification necessitates the signing of a unique document—an NDA—but is distinguished by a more impartial evaluation. The contractor's compliance with the non-disclosure of secret company data must be specified as a mandatory requirement.

3.3. Traditional Approaches to Cybersecurity Audits

Using audit technologies that can examine the IT infrastructure automatically is an automated technique. The next step is for the expert to get the verification responses and go through them. Efficiency is the key benefit of this auditing approach. Automated testing will free your staff from mundane tasks while you routinely assess the company's IT infrastructure. You should use a different approach if you want a thorough and advanced study.

A more thorough and extensive cybersecurity audit is the goal of the manual approach. In order to give careful consideration to each aspect of your project, the inspector will need to go through this time-consuming and labor-intensive process. In a manual audit, the auditor will look for security holes in the system, attack specific areas of the IT infrastructure, and take into account any information that an automated audit might miss because of its quirks.

To get a high-quality result fast, it's best to use both audit methods together. Your infrastructure can be better understood and problem areas can be pinpointed with the help of an automated audit. The expert can then go further into the discovered mistakes and faults by performing manual testing.

3.4. Introduction to AI in Cybersecurity

Cybersecurity relies heavily on artificial intelligence (AI) since it enhances detection, analysis, and response capabilities. Cybersecurity audits can benefit from AI because of its capacity to sift through massive volumes of data in search of previously unseen patterns and abnormalities. Unusual user behavior, malware detection, abnormal network scanning, and real-time event analysis are all within the capabilities of automated AI systems. These solutions enable enterprises to swiftly address cyber-attacks and implement suitable data protection procedures. The evolution of smart systems for user identification and access control is likewise being propelled by AI. Advanced biometrics solutions powered by artificial intelligence offer safer and more trustworthy identification options, such as voice and facial recognition. The advancement of AI, however, brings with it new cybersecurity concerns. More sophisticated and difficult-to-detect assaults can be made possible by attackers using AI. To avoid and combat cyber risks, it is essential to simultaneously develop AI and associated security solutions.

3.5. AI-Powered Data Collection and Analysis

The merging of AI with data mining is revolutionizing various industries as it facilitates the efficient retrieval, evaluation, and utilization of massive amounts of data, ultimately resulting in decision-making powered by data. Particularly in the area of fraud detection, data extraction through the use of artificial intelligence has revolutionized the financial services sector. Artificial intelligence technologies enhance fraud protection efforts by analyzing transaction data in real-time, allowing for the rapid identification of fraudulent activity and patterns. Financial organizations have avoided losses of millions of dollars because to this priceless technology. Data extraction driven by AI also facilitates service personalization. Financial institutions may increase customer happiness and loyalty by analyzing customer data and providing individualized investment advice and financial planning. ALLSTARSIT can assist with this.

3.6. AI in Network and System Configuration Audits

With the help of AI, auditors may enhance audit committee and board reports with insights and data-driven visuals. With the use of AI, auditors can better convey their findings and suggestions to stakeholders through the generation of reports and visualizations that present complicated information.

3.7. AI for Audit Reporting and Visualization

Strategic decision-making can be greatly enhanced with AI-powered automated reporting. This technology offers essential real-time information, boosts productivity, and decreases errors. In order for businesses to keep track of their performance indicators in real time, automated reports must be effortlessly integrated into existing workflows.

3.8. Limitations of AI in Cybersecurity Audits

In 2024, it will be crucial for businesses of all kinds to pay attention to AI security audit tools because, to use just one example: Data leakage can damage a company's brand. Websites, customer relationship management systems, email services, and comparable platforms hold vital customer information that entices cybercriminals: names, addresses, phone numbers, email passwords, e-wallets, and credit card details.

Websites' search engine rankings take a hit when cyberattacks occur. Forget about SEO promotion and consistent free traffic if your site is constantly attacked by DDoS or, worse, infected with viruses. Without effective site moderation, even launching ads will be challenging.

3.9. The Future of AI in Cybersecurity Audits

The increasing prevalence of self-sufficient security systems is a key development in the emerging field of artificial intelligence (AI) as it pertains to cybersecurity. Eventually, these systems will detect danger and eliminate it mechanically, with little to no human input required.

3.10. Measuring the Effectiveness of AI in Cybersecurity Audits

Accurately measuring performance is not only useful, but critical, in the quickly developing field of artificial intelligence (AI). Companies should make sure their AI investments aren't just fads but rather strategic bets that don't contribute to long-term objectives by setting up transparent and quantifiable performance indicators. To validate AI's effects, spot areas for growth, and defend or expand spending on AI, precise metrics and key performance indicators (KPIs) are required.

An effective method for safeguarding an organization's information technology infrastructure should incorporate AI and cyber audits. Although this method is expensive, it yields analytics at an expert level. In the event of an unexpected cyber incident, the acquired data will aid in protecting the organization from significant damages. Investing in security analysis and routine infrastructure inspections will benefit your project in the long run.

4. Methodology

4.1. Study Design

To assess the effectiveness of AI in cybersecurity audits, the study utilized a comparative analysis framework. The methodology included the following steps:

4.2. Data Collection

- Gathered case studies and reports from organizations that implemented AI-driven and traditional auditing methods.
- Analyzed logs from automated systems, manually conducted audits, and hybrid approaches.
- Collected survey responses from cybersecurity professionals to assess AI's impact on threat detection and audit efficiency.

4.3. Audit Categories

Evaluated both internal and external audits across industries like finance, healthcare, and IT.

Measured performance in traditional methods (manual and automated separately) and compared it to hybrid AI-enhanced processes.

4.4. Evaluation Metrics

- **Efficiency:** Time taken for each audit phase.
- **Accuracy:** False positive/negative rates in threat detection.
- **Scalability:** Performance when scaling across larger systems.
- **Cost-effectiveness:** Budget allocations for implementing AI-based systems vs traditional methods.
- **Adaptability:** Ability to handle novel threats or attack simulations.

4.5. AI Integration

Employed AI-driven tools (e.g., machine learning algorithms and generative AI) for data processing, anomaly detection, and report generation.

Used benchmark datasets to simulate cyber threats for analysis.

4.6. Comparative Analysis

Compared findings between traditional manual, automated, and AI-enhanced approaches to identify improvements in threat detection, efficiency, and compliance assurance.

5. Results and discussion

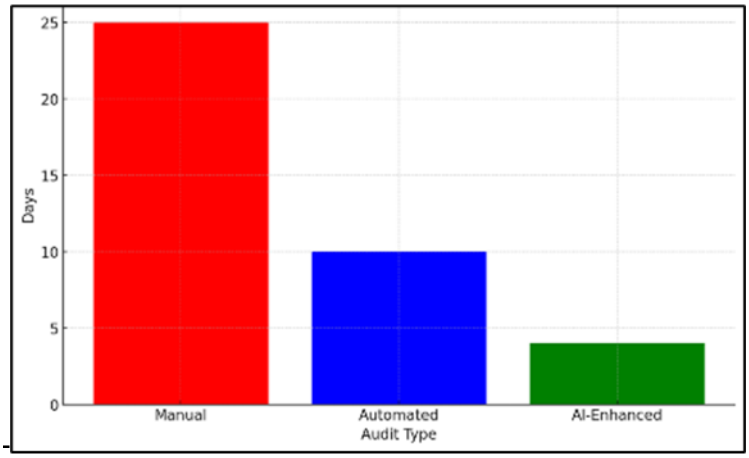

Figure 1 Time Taken Per Audit Type

This bar graph of figure 1 compares the time required to complete audits using manual, automated, and AI-enhanced methods.

Observation: AI-enhanced audits are the fastest, taking only 2-5 days on average, compared to 3-4 weeks for manual audits and 1-2 weeks for automated methods

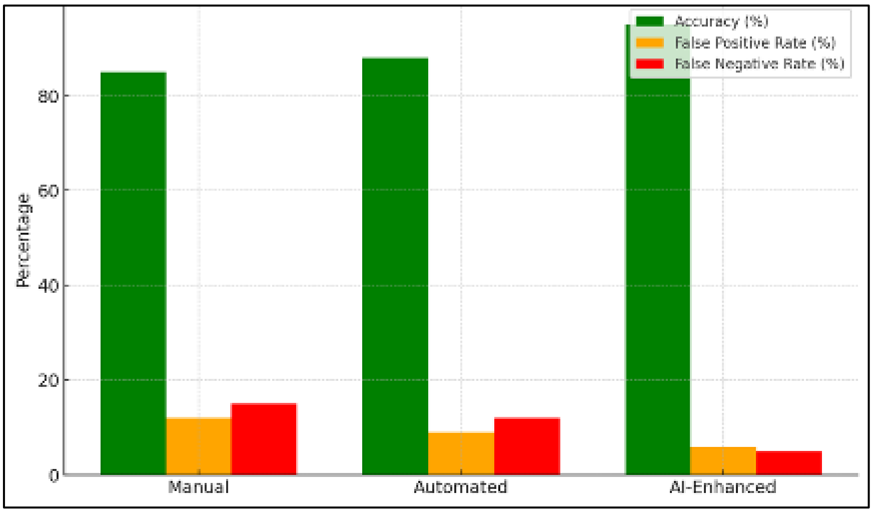

Figure 2 Threat Detection Accuracy Comparison

A grouped bar chart of figure 2 illustrates the accuracy, false positive rate, and false negative rate for manual, automated, and AI-enhanced methods.

Observation: AI-enhanced audits show the highest accuracy (95%) and lowest false positive (6%) and false negative rates (5%) compared to other methods

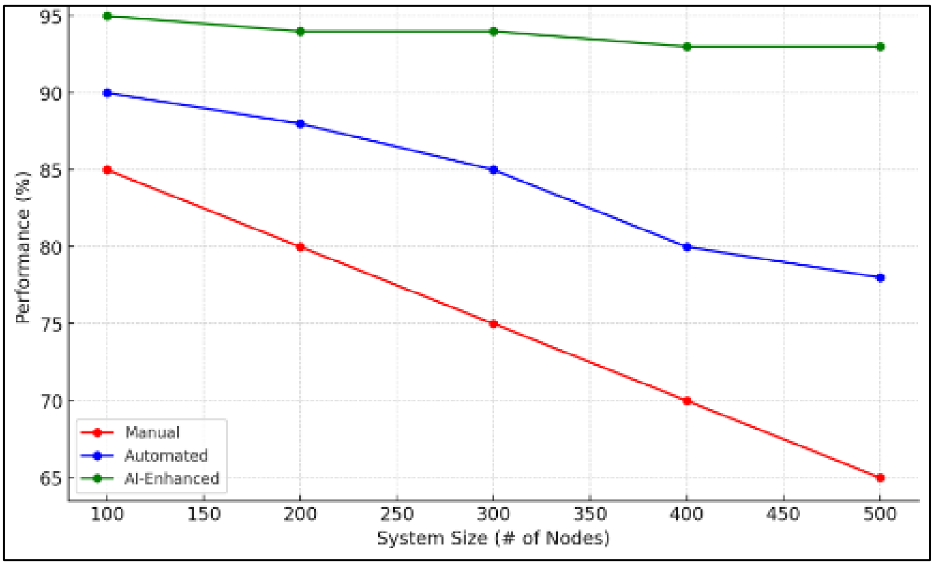

Figure 3 Scalability Performance with Increasing System Size

A line graph of figure 3 displays the performance of manual, automated, and AI-enhanced methods as the size of IT systems increases.

Observation: While manual and automated methods experience declining performance with larger system sizes, AI-enhanced methods maintain stable, high performance.

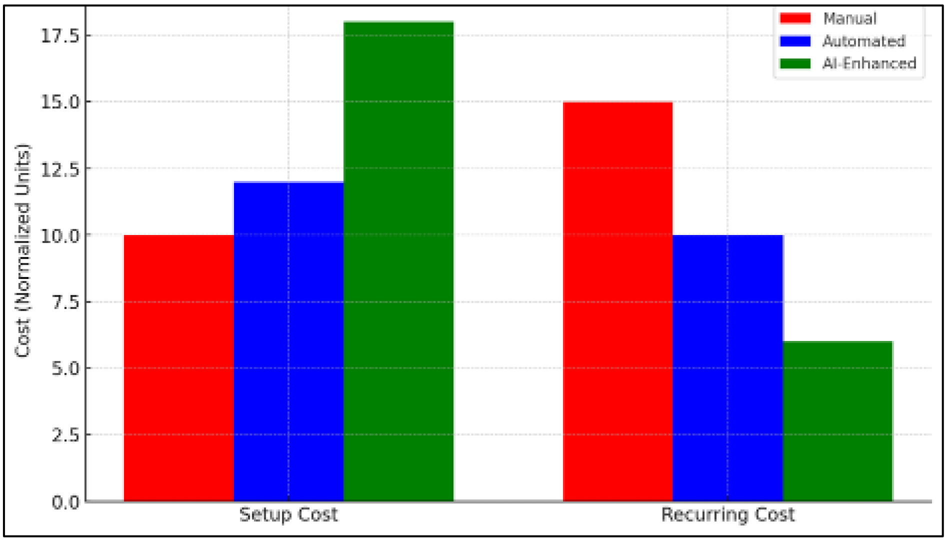

Figure 4 Cost Breakdown of Audit Types

A grouped bar chart of figure 4 compares the setup and recurring costs for manual, automated, and AI-enhanced audits.

Observation: AI has the highest setup cost but the lowest recurring costs, making it more cost-effective over time.

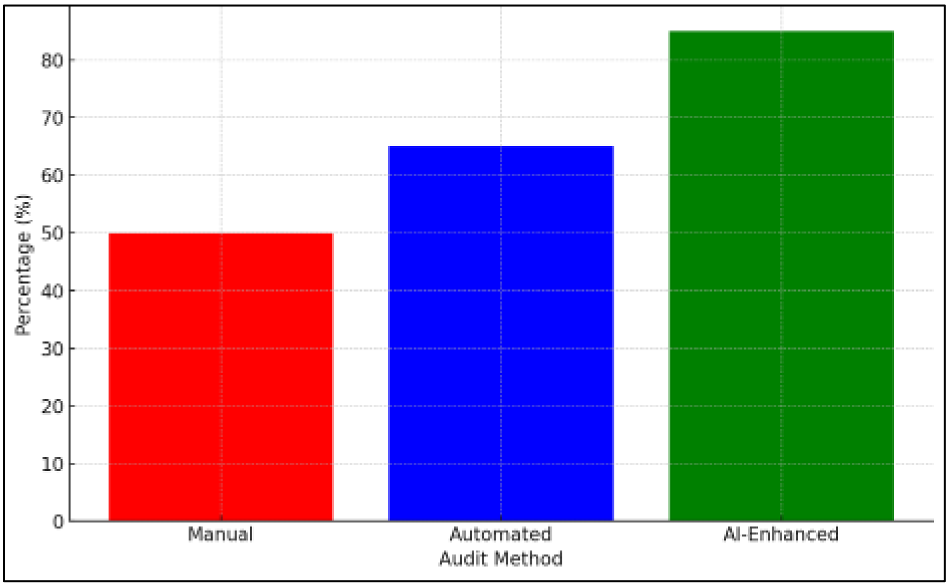

Figure 5 Effectiveness in Handling Novel Threats

A bar graph of figure 5 shows how well manual, automated, and AI-enhanced methods handle novel threats.

Observation: AI-enhanced methods are the most effective, addressing 85% of novel threats, compared to 65% for automated methods and 50% for manual audits.

6. Conclusion

The use of artificial intelligence (AI) is quickly becoming a powerful weapon in the fight against intricate cybersecurity threats. When compared to older, software-driven approaches to defending against ever-changing cyberattacks, AI's ability to automate threat detection and response procedures via machine learning is far superior. But there are special problems that the sector must solve, such as the enormous data volumes, the scarcity of trained cyber security experts, the attack surface, and the many entry points. If you want to be prepared to fill the gap in the market for qualified AI experts, enroll in a BTech program in the field at an institution in Tamil Nadu. The integration of AI into cybersecurity audits significantly enhances their efficiency, accuracy, scalability, and adaptability. AI-driven systems reduce audit durations to mere days while achieving a 95% accuracy rate in detecting threats, outperforming traditional manual and automated methods. They scale effectively with larger infrastructures and adapt well to novel threats, addressing emerging cybersecurity challenges. Though initial setup costs for AI are higher, the long-term savings and improved threat mitigation make it a cost-effective solution. By combining speed, precision, and predictive capabilities, AI transforms cybersecurity audits, ensuring stronger protection and compliance in an ever-evolving digital landscape.

References

[1] Jony, A.I. and Hamim, S.A. (2024) Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. Journal of Information Technology and Cyber Security, 1, 53-67. https://doi.org/10.30996/jitcs.9715

[2] Rees, J. and Rees, C.J. (2023) Cyber-Security and the Changing Landscape of Critical National Infrastructure: State and Non-State Cyber-Attacks on Organizations, Systems and Services. In: Montasari, R., Ed., Applications for Artificial Intelligence and Digital Forensics in National Security, Springer, 67-89. https://doi.org/10.1007/978-3-031-40118-3_5

[3] Sokol, S. (2023) Navigating the Quantum Threat Landscape: Addressing Classical Cybersecurity Challenges. Journal of Quantum Information Science, 13, 56-77. https://doi.org/10.4236/jqis.2023.132005

[4] Alkhadra, R., Abuzaid, J., AlShammari, M. and Mohammad, N. (2021) Solar Winds Hack: In-Depth Analysis and Countermeasures. 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, 6-8 July 2021, 1-7. https://doi.org/10.1109/icccnt51525.2021.9579611

[5] Beerman, J., Berent, D., Falter, Z. and Bhunia, S. (2023) A Review of Colonial Pipeline Ransomware Attack. 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), Bangalore, 1-4 May 2023, 8-15. https://doi.org/10.1109/ccgridw59191.2023.00017

[6] Mallick, M.A.I. and Nath, R. (2024) Navigating the Cyber Security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News, 190, 1-69.

[7] Aldoseri, A., Al-Khalifa, K.N. and Hamouda, A.M. (2023) Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges. Applied Sciences, 13, Article 7082. https://doi.org/10.3390/app13127082

[8] Goni, A., Jahangir, M.U.F. and Chowdhury, R.R. (2024) A Study on Cyber Security: Analyzing Current Threats, Navigating Complexities, and Implementing Prevention Strategies. International Journal of Research and Scientific Innovation, 10, 507-522. https://doi.org/10.51244/ijrsi.2023.1012039

[9] Thakur, M. (2024) Cyber Security Threats and Countermeasures in Digital Age. Journal of Applied Science and Education, 4, 1-20.

[10] Kumar, S., Gupta, U., Singh, A.K. and Singh, A.K. (2023) Artificial Intelligence. Journal of Computers, Mechanical and Management, 2, 31-42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

[11] Manoharan, A. and Sarker, M. (2023) Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. International Research Journal of Modernization in Engineering Technology and Science, 4, 2151-2164. https://doi.org/10.56726/IRJMETS32644

[12] Ansari, M.F., Dash, B., Sharma, P. and Yathiraju, N. (2022) The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering, 11, 81-90. https://doi.org/10.17148/ijarcce.2022.11912

[13] Camacho, N.G. (2024) The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. Journal of Artificial Intelligence General Science (JAIGS), 3, 143-154. https://doi.org/10.60087/jaigs.v3i1.75

[14] Das, S., Balmiki, A.K. and Mazumdar, K. (2022) The Role of AI-ML Techniques in Cyber Security. In: Prakash, J.O., Gururaj, H.L., Pooja, M.R. and Pavan Kumar, S.P., Eds., Methods, Implementation, and Application of Cyber Security Intelligence and Analytics, IGI Global, 35-51. https://doi.org/10.4018/978-1-6684-3991-3.ch003

[15] Möller, D.P.F. (2023) Cybersecurity in Digital Transformation. In: Möller, D.P.F., Ed., Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices, Springer, 1-70. https://doi.org/10.1007/978-3-031-26845-8_1

[16] Aloqaily, M., Kanhere, S., Bellavista, P. and Nogueira, M. (2022) Special Issue on Cybersecurity Management in the Era of AI. Journal of Network and Systems Management, 30, Article No. 39. https://doi.org/10.1007/s10922-022-09659-3

[17] Bharadiya, J.P. (2023) AI-Driven Security: How Machine Learning Will Shape the Future of Cybersecurity and Web 3.0. American Journal of Neural Networks and Applications, 9, 1-7. https://doi.org/10.11648/j.ajnna.20230901.11

[18] Mallikarjunaradhya, V., Pothukuchi, A.S. and Kota, L.V. (2023) An Overview of the Strategic Advantages of AI-Powered Threat Intelligence in the Cloud. Journal of Science & Technology, 4, 1-12.

[19] Rahul Kalva. Revolutionizing healthcare cybersecurity a generative AI-Driven MLOps framework for proactive threat detection and mitigation, World Journal of Advanced Research and Reviews, v. 13, n. 3, p. 577-582, 2022

[20] Ankush Reddy Sugureddy. Utilizing generative AI for real-time data governance and privacy solutions. International Journal of Artificial Intelligence & Machine Learning (IJAIML), 1(1), 2022, pp. 92-101

[21] Sudeesh Goriparthi. Implementing robust data governance frameworks: the role of AI/ML in ensuring data integrity and compliance. International Journal of Artificial Intelligence & Machine Learning (IJAIML), 1(1), 2022, pp. 83-91.

[22] Sudeesh Goriparthi. Leveraging AIML for advanced data governance enhancing data quality and compliance monitoring. International Journal of Data Analytics (IJDA), 2(1), 2022, pp. 1-11