INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY
IJARIIT
ISSN: 2454-132X
Impact Factor: 6.078
*(Volume 11, Issue 5 - V11I5-1187)*
Available online at: https://www.ijariit.com

# The Integration of AI in Cybersecurity

*Abhinav Singh*
*mypublishedpaper@gmail.com*
*Heritage Xperiential Learning School, Haryana*

**ABSTRACT**

***This paper examines the integration of AI in cybersecurity, highlighting its implications for everyday life and its role in preventing cyberattacks. It analyses key protective measures, including SIEM and SOAR, and evaluates the emerging field of Agentic AI as both a potential solution and a risk. Finally, it explores the relationship between AI, IT, and IOT, emphasising AI's capacity to advance technological progress while simultaneously expanding potential vulnerabilities.***

**Keywords:** *AI Cybersecurity, SIEM, SOAR, Agentic AI Cybercrime.*

## INTRODUCTION

"Over the past several years data has become the most valuable resource in the world. This has aided growing interest from individual cybercriminals, APTs, Hacktivists and nation-state actors to steal, modify, destroy information or even cause physical damage."(Podzins and Romanovs 2) "The large-scale growth of the Internet of Things (IoT) in recent years has contributed to a significant increase in fog computing, smart cities, and Industry 4.0, all of which execute the complex data processing of confidential information that must be protected against cybersecurity attacks." (Abdullahi et al. 1) "Verizon - 2018 Data Breach Investigations Report [3] shows that 68% of all identified cyberattacks are discovered month or more after the initial breach. If we take into account that there are high percentage of cyberattacks that are successful and goes undetected, then final percentage would be much higher." (Podzins and Romanovs 2). The majority of personal information and details of a person and institutions are on the Internet. If these get leaked, it could lead to the misuse of the information. Depending on the scale of the attack launched, it could lead to the security of the country or institution being compromised, theft of personal details and terrorism. The prevention of these attacks and the protection of information are what cybersecurity measures are. Cybersecurity in other terms is "the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" ("What is Cybersecurity?") "Early work examining the cybersecurity institutional landscape was descriptive, identifying international/regional governmental, public-private and non-governmental organisations active in cybersecurity." (Portnoy and Goodman as quoted in Kuerbis and Badiei 2) The initial research on cybersecurity institutions mainly focused on the different types of organizations involved - international and regional governments, public-private partnerships and non-governmental groups - that play an active role in cybersecurity. The studies aimed to map out who was active in the field of cybersecurity, laying the groundwork for deeper analysis by highlighting the diversity and scope of institutional involvement across different sectors and levels of government. "Cybersecurity attacks have increased rapidly in various domains, such as smart homes, healthcare, energy, agriculture, automation, and industrial processes." (Abdullahi et al. 1) This increase is driven by the shifting of the vast majority's reliance on digital technologies, which has increased attack vulnerability. As more and more devices and systems become a part of the Internet of Things (IoT), the more vulnerable the security and safety of institutions and countries are. "Institutional landscape of cybersecurity is more of a patchwork of efforts rather than an overarching landscape that addresses all the known cyber threats." (Kuerbis and Badiei 3) Although many governments, private companies, and international organizations are working to improve cybersecurity, their efforts are often disconnected and lack coordination. This leads to overlapping responsibilities, different rules across different regions, and gaps in how cyber incidents are managed. As technology evolves, it becomes even harder for institutions to keep up with the new threats. Without a more united and cooperative approach, both individuals and systems remain exposed to risks such as hacking, identity theft, and other cyberattacks. "IoT comprises interconnected devices that are increasingly developed on a large scale, taking into account various characteristics through cloud and fog computing, where the processing of real-time applications can be enhanced" (Abdullahi et al. 2) With the tremendous growth on the dependence on IoT and the emergence of AI as part of the fourth industrial revolution (Industry 4.0), the security of its users has also been compromised tremendously in the form of cyber attacks. AI can be a threat as well as a solution to cybersecurity. For example, "criminals, bad state actors, unscrupulous competitors, and inside threats that will manipulate their companies' fledgling AI programs. The second risk is that attackers will use AI in various ways to exploit vulnerabilities in their victims' defences." (Goosen et al. 1) Furthermore, attackers have easy access to malware and identity theft kits, which are easy to find and inexpensive to buy, making it much easier to carry out a cyber-attack. On the positive side, by optimising the proper use of AI, companies can streamline and improve the security operating model by reducing time-consuming and complex manual inspection and intervention processes and redirecting human efforts to supervisory and problem-solving tasks. "AI can also provide insights into sources of potential threats from internal and external sensors or small pieces of monitoring software that evaluate digital traffic by performing deep packet inspection." (Goosen et al. 3)

## PREVENTION OF CYBER ATTACKS

"Tens of millions of cyber-attacks (Emails, online transactions, live video streaming, online games, and navigation are all examples of fraudulent Internet-based intelligence gathering) are launched every day against Internet users throughout the world" (Vakil and Swaminarayan 1). There are measures in place that help in the prevention of these attacks. These include network security measures such as Firewalls (which act as a barrier between internal networks and external threats by filtering traffic), Intrusion Detection Systems (which monitor network traffic for suspicious activity and take actions when threats are detected), and Segmentation (dividing the network into zones to limit lateral movement by attackers). Furthermore, there should be regular security audits and penetration testing so that we can identify vulnerabilities before attackers do. These audits should include Risk Assessment, which helps prioritise potential risks and threats to the IT infrastructure. At present, the techniques that cyber attackers use to facilitate these attacks are related to exploiting human feelings; thus, the most necessary way to overcome these attacks is to spread awareness related to this topic. Other attacks include phishing attacks (attacks that trick users into giving up sensitive information via fake emails, messages or websites), and banking trojans (which can cause interference with legitimate banking transactions and may result in the theft of money and important credentials). Some common methods to prevent these attacks include enabling two-step verification and signature-based security that can help protect your device. To overcome these threats, several researchers have developed IDSs (Intrusion Detection Systems) based on various AI approaches. "(Kurte et al.), for example, introduced a distributed service framework that supports the development of trustworthiness and privacy protection for multidirectional data aggregation for edge computing enhancement. (Diro and Chilamkurti) proposed a detection system using deep learning (DL) methods to detect cybersecurity attacks in IoT. They compared the DL model with traditional machine learning (ML) approaches. (Farivar et al). identified AI for the detection of malicious attacks in CPS and IIoT and proposed a hybrid intelligent classic control approach for the reconstruction of cyberattacks on the input data of non-linear CPS through shared networks." (Abdullahi et al. 2). Therefore, ongoing investment in AI-based detection systems, public education, and adaptive security protocols is critical to staying ahead of cybercriminals and protecting individual and organisational data.

## SIEM and SOAR

SIEM (Security Incident and Event Monitoring) is a software solution that helps detect, analyze, and respond to potential security threats before they cause harm. "Firewalls, intrusion detection system, intrusion prevention system, Distributed Denial of Service protection solutions and other security solutions look for malicious activity at various points within the IT infrastructure, from the perimeter to endpoints." (Podzins and Romanovs 2) "SIEM is a solution which analyzes events/logs from each of the security solutions." (Podzins and Romanovs 2) "Best of all this and other defensive actions can be automated which gives a company 24/7 reactive security solution which learns from entire IT environment and using context performs high probability remediation actions. Using this method is also the best way to detect Zero-day attacks." (Podzins and Romanovs 2). Further, we will now delve into the advantages that SIEM has to offer.

i. Analysis of a large number of files, which will allow detection of various threats such as ransomware, intrusion attempts, DDoS attacks, etc.
ii. "Information on historical events for forensic purposes. In the same time conserving audit log integrity." (Podzins and Romanovs 4)
iii. Increased incident response efficiency

Apart from all these benefits, SIEM has some disadvantages as well. These include:

i. Costliness of the whole system - initial purchase price, including licensing costs, which is affected by the number of log files
ii. Low availability of employees who actually know how to operate the system properly.
iii. Requires a high amount of maintenance to investigate alerts
iv. Does not work without other security solutions such as firewalls, IPS/IDS, etc.

## SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)

"The Soar architecture has been used extensively, both for developing AI applications and cognitive models. One of its strengths has been the ability to efficiently represent and use large bodies of symbolic knowledge to solve a wide variety of problems using many different methods. It dynamically combines available knowledge for decision-making, and can dynamically create subgoals whenever the knowledge for a decision is incomplete or inconsistent." (Nason and Laird 1) The SOAR architecture is widely used in AI and cognitive modelling because it effectively handles large symbolic knowledge, applies diverse problem-solving methods, dynamically integrates knowledge for decisions, and generates subgoals where knowledge is inconsistent or incomplete. "Soar has strengths in knowledge-rich symbolic reasoning and learning and weaknesses in knowledge-lean, statistical-based learning. Soar allows both symbolic and numeric preferences to contribute to the decision. Thus, it is possible to encode control knowledge that one option is better than another." (Nason and Laird 57) "The utilities captured by the numeric preferences in Soar do not rely solely on the idea of progress toward a goal, but instead are associated with a more flexible reward function. This reward function is capable of representing goal-directed activity, but can also be used for ongoing activities, such as the top level of an agent, which monitors energy levels or selects goals to be pursued." (Nason and Laird 57) "Soar distinguishes between the conditions for when an action/operator is valid and when it is desirable, which in turn gives it a richer representation for capturing complex reward/utility functions."

### Benefits and privacy concerns of integrating AI in everyday life

Integrating AI into everyday life - from hospitals to classrooms and digital assistants - brings transformative benefits: more precise diagnostics, adaptive personalised learning, and seamless workflows. However, this comes with many risks and consequences as well. "Most companies have implemented protocols for when an employee emails confidential information to the wrong person. A new version of that problem occurs when an employee uploads sensitive information to a consumer (i.e., not enterprise) AI tool" (Gesser et al.). "Each AI provider is different in how it treats confidential information that is uploaded to its consumer tools, and often there are differences among the various tools from the same provider." (Gesser et al.) Thus, the most crucial first step is to identify the platform to which one has uploaded sensitive or confidential information.

To further reduce the risk "the company should take steps to contain the impact of the event. Depending on the platform involved, the data affected, and the potential obligations" (Gesser et al.) This can be done by:

"**Account settings adjustments.** The company should work with the employee to determine what privacy and security controls the employee had enabled on their account and choose the most secure options, if they were not already selected. Changing these settings may result in the data not being used for analytics and model training purposes.

**Deletion.** Depending on the platform, deleting a user's interaction history (and in some cases, the entire account) will delete the uploaded data from the provider's servers. AI providers' policies often contain details about how the deletion process works and how long it may take for the deletion to occur.

**Outreach.** The company should consider whether contacting the AI tool's provider will help delete the uploaded data. The decision to reach out should depend on where the provider is located and whether they have some formal or informal process for notification and remediation of accidentally uploaded confidential data." (Gesser et al.)

In conclusion, while AI promises proficiency and efficiency in everyday tasks, users may not realise that private inputs - medical records, student essays, diet plans, etc.- could be retained, mined, or exposed. Thus, clear rules, honest handling of data, and security measures help us reap the benefits of AI integration safely.

## AGENTIC AI IN CYBERSECURITY (PROS AND CONS)

"Agentic AI can transform cybersecurity practices by automating and enhancing threat detection, response, and mitigation. By leveraging machine learning and adaptive algorithms, agentic AI systems can continuously monitor network traffic, identify suspicious patterns, and predict potential vulnerabilities before they are exploited. These systems can autonomously adapt to new threats in real-time, providing a more dynamic defense mechanism that outpaces traditional, human-driven approaches. Additionally, agentic AI can be deployed in incident response, making immediate decisions and executing predefined actions to neutralize threats, thereby reducing the impact of attacks and improving the overall efficiency of cybersecurity operations." (Kshetri 7) Agentic AI refers to systems designed to complete specific tasks with little human oversight. These systems are made up of intelligent agents that solve problems in real time by making decisions like humans. In setups with multiple agents, each focuses on a particular part of the task to help achieve the overall goal. "Amid a vast well-established body of research on cybersecurity and on the application of AI to cybersecurity, the literature on agentic AI approaches to cybersecurity is disjointed and partial." (Maka et al. 2). Although there is a large and well-developed body of research on cybersecurity and the use of AI in the field, studies specifically focusing on Agentic AI approaches to cybersecurity remain incomplete. "Various preventive mechanisms have been adopted from time to time to safeguard the world from the wrath of these cyber predators; however, past records of cyber-attacks and malware outbreaks show that such incidents have been increasing at an alarming rate in terms of volume and sophistication too. As a counter-response mechanism, automated, intelligent, and self-sufficient reactive systems are sought as a panacea. As an attempt to make this happen, Agentic AI has found its application gracefully in the cyber world to come up with contrasting policies against the malicious agent in the cyber world." "Unlike traditional AI systems that function within controlled environments, AI agents interact with various systems and external data sources, expanding the potential attack surface. This can lead to unauthorized access, data leakage, and other vulnerabilities. Weak integration or system flaws have previously allowed sensitive data to be exposed, while malicious actors or coding errors can manipulate AI agents, causing unintended disruptions or financial losses (Ramesh, 2025). If an agentic AI system is hacked, the consequences can be severe. First, detecting and confirming the breach may take time, and even a minor change can lead to significant effects." (Kshetri 2) AI systems that operate independently and connect with outside platforms face a higher risk of cyberattacks. Because they access multiple networks, they become an easy target for attackers. As these AI systems contain information from various platforms, a breach may result in major problems or even financial damage. Furthermore, these breaches are harder to find, thus even tiny repercussions can cause major ripple effects. Despite various preventive measures, cyberattacks and malware continue to rise in quantity and quality. In response, there is a need for automated, intelligent, and self-sufficient systems. Agentic AI has emerged as a promising solution, offering various countermeasures against cyberattacks.

## HOW AI RELATES TO IT/IOT

### AI in IT:

Information Technology (IT) refers to the systems and infrastructure used for storing, retrieving, processing, and transmitting data. It includes:

Hardware: computers, servers, networks, storage devices

Software: databases, operating systems, enterprise applications

AI is essentially a layer of intelligence added to the IT infrastructure. Instead of storing and transferring data, AI enables IT systems to learn, analyse, and make decisions. AI can enhance and simplify the working of the IT infrastructure in the following ways:

1. "Incident Response Gets an Upgrade
   When a problem arises, engineers often must search through a mountain of log files, dashboards, and monitoring tools to understand what went wrong. This process is time-consuming and worse at times, inconclusive. Gen AI can transform the tedious process; it can now scan logs, interpret error patterns, and summarize probable root causes within minutes. Instead of spending hours on diagnostics, teams can move straight to remediation. AI-based incident response even suggests fixes based on historical resolutions, freeing engineers from low-level triage." (Somani)
2. "Predicting Failures Before They Happen
   While system failures are costly, they often display signs of trouble early on. This could be in the form of CPU spikes, disk read errors, or network latency. Gen AI models can now learn from these signals and predict potential failures before they escalate. This isn't science fiction. Trained in historical telemetry data, these systems can alert engineers about probable issues with time to intervene. The best part is that these aren't just vague warnings. Predictive maintenance using Gen AI can explain why it believes a failure may happen and which component is most likely involved." (Somani)
3. "Smarter Capacity Planning
   Traditional forecasting infrastructure needs used to be about gut feelings and static reports. Today, Gen AI brings intelligence to planning.

By analyzing past usage trends, business growth projections, and even external events like product launches or seasonality, Gen AI can produce draft capacity reports. Engineers need only to refine these reports and save hours of manual work. These forecasts also help reduce overprovisioning while at the same time ensuring critical workloads are supported by an adequate number of resources. This marks a shift toward AI for capacity planning." (Somani)

4. "Better Control Over Configuration Drift
   Drift happens when changes sneak into systems without being reflected in infrastructure-as-a code templates. Over time, this introduces risk, misalignment, and outages. AI-powered configuration management tools can now compare current system states against approved configurations and flag mismatches. Some tools even suggest updates or pull requests to sync everything back up. Rather than manually inspect environments, engineers can review Gen AI generated drifts and take action quickly." (Somani)

In conclusion, AI makes IT smarter, proactive, and capable of decision-making, rather than just being a storage and processing system.

## AI IN IOT

IOT "can be best understood as a network of digital and analog machines and computing devices provided with unique identifiers (UIDs) that have the ability to exchange data without human intervention. In most cases, this manifests as a human interfacing with a central hub device or application, often a mobile app, that then goes on to send data and instructions to one or multiple fringe IoT devices." (Kuzlu et al. 1) "The IoT concept has given the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability in terms of device connectivity. However, IoTs are vulnerable to cyberattacks due to a combination of their multiple attack surfaces and their newness and thus lack of security standardizations and requirements." (Kuzlu et al. 1) Thus, AI can be used to prevent these cyberattacks.

## CONCLUSION

This research paper took an in-depth view of the growth of IOT and AI and their integration in Cybersecurity and everyday life over the past few years, which is driven by the shifting of the vast majority's reliance on digital technologies. It also looks into how AI has proven to be both beneficial and harmful, as it brings transformative benefits: more precise diagnostics, adaptive personalised learning, and seamless workflows. However, this comes with many risks and consequences as well, since employees can upload sensitive content or confidential data, which can be hacked, mined, or exposed. This is especially crucial for a complex domain like cybersecurity, where adoption of new technology comes with multifold implications. There are tens of millions of cyberattacks that are launched every day against internet users. However, there are measures in place that help prevent these attacks. These measures include SIEM (Security Incident and Event Monitoring), which is a software solution that helps detect, analyze, and respond to potential security threats before they cause harm, however it's downsides include the costliness of the whole system - initial purchase price, including licensing costs, which is affected by the number of log files and the low availability of employees who actually know how to operate the system properly. Another measure is SOAR (Security Orchestration, Automation, and Response), which is widely used in AI and cognitive modelling because it effectively handles large symbolic knowledge, applies diverse problem-solving methods, dynamically integrates knowledge for decisions, and generates subgoals where knowledge is inconsistent or incomplete. Even though SOAR has strengths in knowledge-rich symbolic reasoning and learning, and weaknesses in knowledge-lean, statistical-based learning. It is necessary to invest in these measures to stay ahead of cybercriminals and protect individual and organisational data. Furthermore, the vast implications of AI can be seen in its everyday usage, which helps make our lives easier. This very absorption of data and ease in everyday life is what makes AI susceptible to human errors, such as uploading of sensitive content and sharing of confidential information. AI itself has also grown over the past few years, with the introduction of new systems like agentic AI, which can now do almost any task imaginable, such as booking a plane ticket, to even placing orders from your favourite restaurant. However, these tasks require a lot of personal data, from banking details to your home address. This amount of data in the hands of AI causes great concern as it can be hacked, retained, or exposed. This gives ground for further research to be done to make sure it is almost impossible to hack AI systems.

## REFERENCES

[1] Abbas, Hafiz Syed Mohsin, et al. "Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare." Edited by Maurizio Naldi. *PLOS ONE*, vol. 17, no. 11, 2022, p. 13. *Public Library of Science (PLOS)*, https://doi.org/10.1371/journal.pone.0274550.

[2] Abdullahi, Mujaheed, et al. "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review." Edited by Qusay H. Mahmoud. *Electronics*, vol. 11, no. 198, 2022, p. 27, https://doi.org/10.3390/electronics11020198.

[3] Cheng, Eric C.K., and Tianchong Wang. "Institutional Strategies for Cybersecurity in Higher Education Institutions." Edited by Sherali Zeadally. *Information*, vol. 13, no. 4, 2022, p. 14. *MDPI*, https://doi.org/10.3390/info13040192.

[4] Gesser, Avi, et al. "An Employee Just Uploaded Sensitive Data to a Consumer AI Tool – Now What?" *Debevoise & Plimpton*, 2025, https://www.debevoisedatablog.com/2025/04/16/an-employee-just-uploaded-sensitive-data-to-a-consumer-ai-tool-now-what/. Accessed Monday September 2025.

[5] Goosen, Ryan, et al. "Artificial Intelligence is a threat to Cybersecurity. It's also a solution." *BCG (Boston Consulting Group)*, 2018. *Google Scholar*, https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.

[6] Kshetri, Nir. "Transforming cybersecurity with agentic AI to combat emerging cyber threats." *Telecommunications Policy*, vol. N/A, no. N/A, 2025, p. 12. *Science Direct*, https://www.sciencedirect.com/science/article/pii/S0308596125000734.

[7] Kuerbis, Brenden, and Farzaneh Badiei. "Mapping the Cybersecurity Institutional Landscape." *SSRN (Social Science Research Network)*, vol. Not applicable, no. Not applicable, 2021, p. 33. *SSRN (Social Science Research Network)*, https://ssrn.com/abstract=3891296.

[8] Kuzlu, Murat, et al. "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity." *Discover*, vol. 1, no. 7, 2021, p. 14. *Springer Nature*, https://link.springer.com/content/pdf/10.1007/s43926-020-00001-4.pdf.

[9] Maka, Srinivasa Rao, et al. "Automating Cyber Threat Response Using Agentic AI and Reinforcement Learning Techniques." *Journal of Electrical Systems*, vol. 17, no. 4, 2021, p. 11, https://pdf.sciencedirectassets.com/271735/1-s2.0-S0308596125X00069/1-s2.0-S0308596125000734/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEID%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJGMEQCIEkriLoZnRq%2FSt%2FtJCG6pWITMAAK%2FYq8UBBmvlDR8Hh0AiAGYB4y257.

[10] Nason, Shelly, and John E. Laird. "Soar-RL: integrating reinforcement learning with Soar." *Cognitive Systems Research*, vol. 6, 2005, pp. 51-59. *Google Scholar*, https://doi.org/10.1016/0004-3702(87)90050-6. Accessed 11 08 2025.

[11] Podzins, Oskars, and Andrejs Romanovs. "Why SIEM is Irreplaceable in a Secure IT Environment?" *Research Gate*, 2021, pp. 1-6. *IEEE*, https://ieeexplore.ieee.org/abstract/document/8732173. Accessed 11 08 2025.

[12] Somani, Ankur. "How Generative AI Is Transforming IT Infrastructure Management - Calsoft Blog." *Calsoft Inc*, 25 July 2025, https://www.calsoftinc.com/blogs/how-generative-ai-is-transforming-it-infrastructure-management.html. Accessed 20 September 2025.

[13] Stryker, Cole. "What Is Agentic AI?" *IBM*, https://www.ibm.com/think/topics/agentic-ai. Accessed 30 July 2025.

[14] Vakil, Jigar, and Dr. Priya Swaminarayan. "Cyber Attacks: Detection and Prevention." *IJSRSET*, vol. 9, no. 5, 2022, p. 12. *8605-libre.pdf*, https://d1wqtxts1xzle7.cloudfront.net/96457680/8605-libre.pdf?1672204779=&response-content-disposition=inline%3B+filename%3DCyber_Attacks_Detection_and_Prevention.pdf&Expires=1750263682&Signature=bQjwGkz~rEcY2Y72JHbxlzO-yIpCvtxi8EgsMDuJoAlvgGcUCUBuYxbEmxa8.

[15] "What is Cybersecurity?" *CISA*, 1 February 2021, https://www.cisa.gov/news-events/news/what-cybersecurity. Accessed 2 June 2025.