International Journal of Business Integrity and Technology Advancements (IJBITA)

Volume – 02
Issue – 01
(2026)

# Cybersecurity Risk Management in Smart IoT Ecosystems Using Artificial Intelligence

Nolan Gael, Department of Computer Science and Engineering, Wright State University
nolangael@writesate.edu

***Article Info:***
***Received: 28 Dec, 2025***
***Processed: 20 Jan, 2026***
***Published: 03 Feb, 2026***

***Keywords:*** *Artificial Intelligence, Cybersecurity Risk Management, Internet of Things, Smart Ecosystems, Machine Learning, IoT Security, Threat Detection, Zero Trust Architecture, Predictive Analytics, Smart Devices.*

## ABSTRACT

Faster evolution of IoT (Internet of Things) has changed the course of today's digital world fostering the interconnection of smart devices, intelligent automation, and real-time data sharing across various industries. Smart IoT ecosystems are becoming more and more embedded in healthcare, transportation, manufacturing, smart cities, energy infrastructures, retail and industrial. Internet of Things (IoT) technologies offer operational efficiency, scalability and automation, but they also bring with them many cybersecurity problems, such as a wide attack surface, weak authentication mechanisms, insecure communication protocols, device heterogeneity and resource constraint. Traditional cyber-security approaches are not enough to deal with the highly dynamic and complex cyber threats directed to the IoT infrastructure. Thus, organizations have turned to adopting artificial intelligence (AI) powered cybersecurity risk management frameworks for enhanced threat detection, predictive analytics, anomaly identification, incident response and resilience.

This review article presents a critical analysis of Cyber Security Risk Management in smart IoT ecosystem through AI. It delves into IoT cybersecurity concepts, AI-powered threat detection systems, machine learning applications, behavioral analytics, smart intrusion detection systems, predictive risk management, blockchain integration, cloud–edge security models, and Zero Trust security models. In addition, the article covers some of the most significant cyber threats to IoT, such as botnets, ransomware, DDoS, data breaches, insider threats, and AI-driven attacks.

The study highlights the importance of machine learning, deep learning, reinforcement learning, natural language processing and federated learning in the context of AI technologies for boosting IoT security infrastructures. All the ethical issues, privacy concerns, threat from malicious AI, workforce concerns and regulations are explored in depth. Moreover, innovations that are new to the industry, such as digital twins, explainable AI, autonomous security systems and quantum-resistant cybersecurity, are all mentioned.

Results of the analysis show that the use of AI in cybersecurity risk management greatly contributes to the security, resilience, and adaptability of smart IoT ecosystems. But to make them work successfully, it is important to have robust governance structures, ethics committees, human-AI partnerships, and ongoing supervision. The authors conclude that cybersecurity strategies leveraging AI are crucial for safeguarding modern smart ecosystems and promoting sustainable digital transformation.

**Corresponding email:** nolangael@writesate.edu

## INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most game-changers in the modern digital era. IoT is a network of connected physical devices, sensors, software application, and communication systems, which gather, process and share data over the internet [1]. Smart IoT ecosystems are found increasingly more in health care systems, in industrial automation, in transportation systems, in smart cities, in energy infrastructures, in agriculture technologies, in retail systems, and in consumer applications [2]. The swift development of IoT technologies contributes to a faster digital transformation and opens the doors to the possibilities of intelligent automation, real time monitoring, predictive maintenance and operational optimization [3].

With the development of IoT ecosystem billions of interconnected things are producing huge amount of data [4]. intelligent devices constantly interact with cloud-based platforms, edge computing systems, and enterprise networks to enable intelligent decision-making and automation services [5]. This interconnected nature has, however, come with its own cybersecurity problems.

IoT devices are also prone to low computing power, weak authentication mechanisms, out-of-date firmware and insecure communication protocols. In smart devices, a lot of devices are made to be functional and budget-friendly instead of being cybersecurity resilient [6]. Thus, cybercriminals are increasingly taking advantage of weaknesses in the IoT system to conduct ransomware attacks, botnets, distributed denial-of-service (DDoS) attacks, data breaches and cyber espionage [7].

Today's IoT environments are many layered and have created a vast attack surface of the organization [8]. The distributed and dynamic nature of IoT environment makes the conventional cybersecurity models that focus on perimeter defense strategies inadequate [9]. The operation of smart ecosystems requires them to support heterogeneous devices, multi-cloud architectures, edge computing systems, wireless communication protocols and real-time data exchanges, which pose complex management issues in terms of security [10].

In the world of IoT cybersecurity risk management, Artificial Intelligence (AI) is a game-changer. AI technologies can be used to analyze vast amounts of information, detect patterns in incidents, automate incident response protocols and predict attacks [11]. Algorithms for machine learning, deep learning, behavioral analytics and natural language processing systems are increasingly being used in security related to IoT [12].

AI-powered cybersecurity solutions offer a range of strategic benefits to IoT ecosystems. These systems also have the ability to monitor the actions of these devices continuously and recognize any abnormal activity, detect malware, analyze the pattern of network traffic and automate the risk mitigation measures [13]. AI technologies can also help in implementing predictive analytics, which can help organisations to foresee and prioritise vulnerabilities to threats [14].

AI in IoT cybersecurity is particularly notable because of the amount of real-time data generated and analyzed in IoT systems, which is too much for traditional security measures to handle [15]. In many cases, suspicious activities can be identified in real-time with the help of AI analytics, which helps to reduce the time needed to react to cyber incidences [16].

All these advantages come with certain challenges for AI adoption in IoT cybersecurity. In addition to algorithmic manipulation attacks, AI systems can be targets of adversarial attacks and data poisoning attacks [17].

Furthermore, challenges like privacy and ethics, the availability of skilled staff, and regulatory uncertainties remain in the field of implementing AI in smart ecosystems. This is a review article on Cyber Security risk management in smart IoT ecosystem with AI. The paper provides the foundations of IoT cyber security, AI-based cyber security frameworks, major IoT cyber security threats, smart strategies to manage cyber risks, organizational models for implementation, ethical considerations, and research directions.

## UNDERSTANDING SMART IOT ECOSYSTEMS AND CYBERSECURITY RISKS

### A. SMART IOT ECOSYSTEMS

Smart IoT ecosystems are comprised of a group of interconnected devices, sensors, communication networks, cloud infrastructures and intelligent applications that share data and intelligence to enable automated and intelligent operations. These ecosystems combine physical and digital components, which add value to the efficiency, monitoring and decision making for a number of sectors. The use of smart IoT systems is seen all around various fields such as healthcare, manufacturing, transportation, smart cities, agriculture, smart homes, energy infrastructures, retail systems, and logistics networks [19].

**Corresponding email:** nolangael@writesate.edu

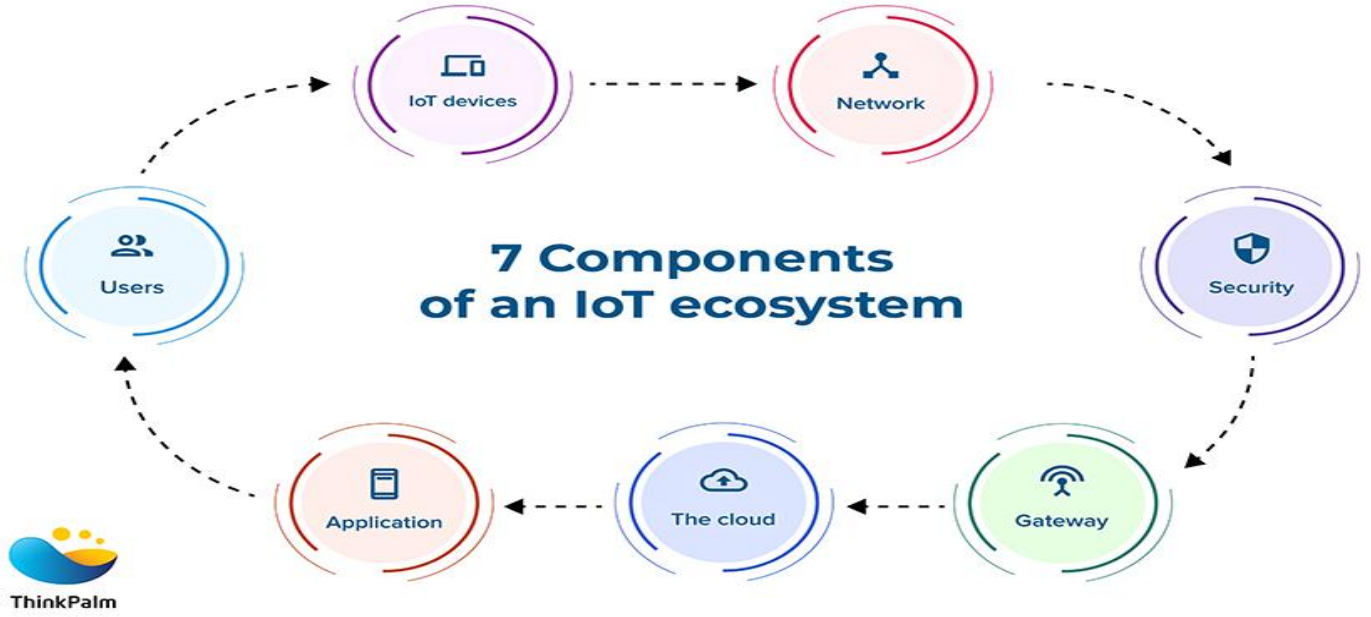


**Fig 1:** 7 components of an IoT ecosystem

Such environments are characterized by persistent connectivity, extensive data sharing, distributed computing architectures and device-to-cloud communication in real-time [20]. Today, the central role of interdependent technologies has established very fluid ecosystems that can support automation, predictive analytics, and intelligent operational management.

**B. CYBERSECURITY RISKS IN IOT ENVIRONMENTS**

Due to their distributed nature, heterogeneous device environments and large attack surfaces, IoT ecosystems are subject to many cybersecurity threats. Many IoT devices have low computing power and have poor security measures, which can be exploited [21]. These are issues such as vulnerary authentication, insecure API, lack of firmware updates, poor encryption techniques, insecure communication protocols, device misconfigurations, insider threats, and supply chain vulnerabilities [22].

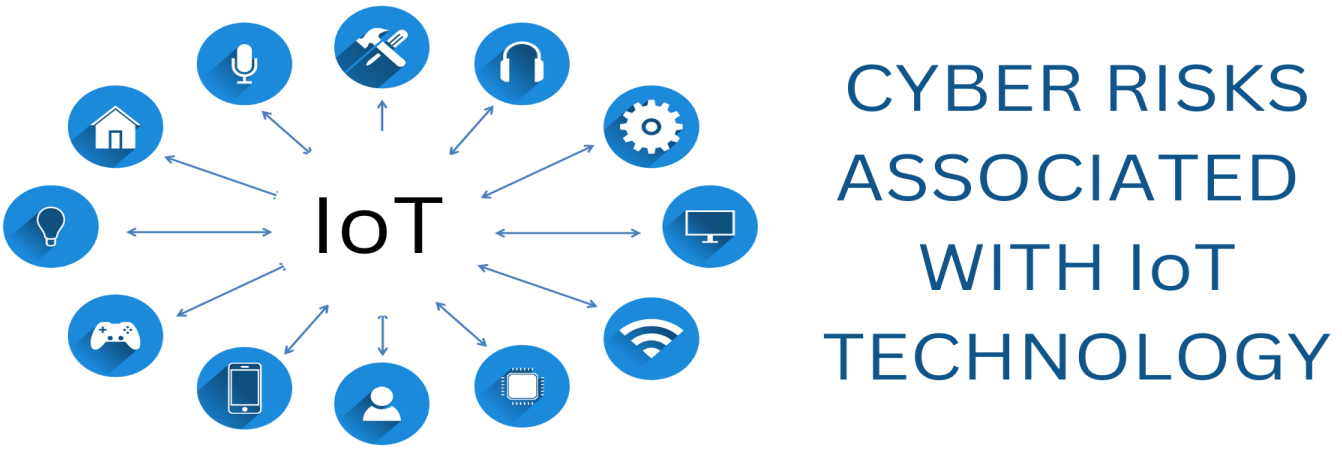


**Fig 2**: Cyber Risks in IoT Envorement

Corresponding email: nolangael@writesate.edu

The rapid proliferation of connected devices has boosted organizational vulnerability to cyber threats, and allowed cybercriminals to find opportunities to exploit vulnerable smart infrastructures.

### C. MAJOR CYBER THREATS AFFECTING IOT ECOSYSTEMS

The vulnerabilities of smart IoT ecosystems within the cyber realm span across various types of potential threats, which can be harmful in a number of ways, disrupting operations, compromising sensitive information and affecting critical infrastructures. One of the most prevalent attacks is botnet attacks: compromised IoT devices are employed together to conduct distributed denial-of-service (DDoS) attacks [23]. The insecurity of IoT devices was illustrated by the destructive power they can show in global cyber attacks, like the Mirai malware [24]. Smart Healthcare systems, industrial infrastructures, and connected networks are vulnerable to such ransomware attacks, which can cause significant disruptions to essential services and continuity of operations [25]. Data breach is also an issue of big concern as IoT ecosystems are processing sensitive information such as personal, industrial and operational [26]. Furthermore, the presence of insider threats and authorised insider access is still present in smart ecosystems cyber incidents [27]. The cyber threat landscape has evolved further and now includes threats that are increasingly more complex and can be carried out more efficiently with AI techniques to evade detection [28-29].

### I. CYBERSECURITY RISKS IN IOT ENVIRONMENTS

Many challenges arise in the realm of cybersecurity in an IoT ecosystem owing to its distributed and diversified devices [30].

Major cybersecurity vulnerabilities include:

- Weak authentication mechanisms
- Insecure APIs
- Lack of firmware updates
- Poor encryption standards
- Insecure communication protocols
- Device misconfigurations
- Insider threats
- Supply chain vulnerabilities

The proliferation of connected devices now creates more points of attack and potential for cyber exploitation within organisations.

### D. MAJOR CYBER THREATS AFFECTING IOT ECOSYSTEMS

### I. BOTNET ATTACKS

IoT devices are often the victims of botnet attacks. Attackers have shown that it is possible to take advantage of malicious IoT devices to conduct massive DDoS attacks, as happened with Mirai.

### II. RANSOMWARE

Smart healthcare systems, industrial networks and connected infrastructures can be vulnerable to ransomware attacks that can impact critical services and operations.

### III. DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS

The attack leverages on weak IoT devices to flood networks and cause services disruption.

### IV. DATA BREACHES

IoT ecosystems host sensitive personal, operational and industrial information, which makes them a tempting target for cybercriminals.

### V. INSIDER THREATS

Unauthorized internal access and human error still play a large part in IoT security incidents.

### VI. AI-POWERED CYBERATTACKS

This is because cybercriminals are increasingly leveraging AI technologies to make attacks more automated, circumvent security measures, and exploit vulnerabilities with greater efficacy.

## ARTIFICIAL INTELLIGENCE IN IOT CYBERSECURITY

### A. ROLE OF AI IN CYBERSECURITY RISK MANAGEMENT

AI has become a key technology in the smart IoT ecosystems to address cybersecurity threats [31]. AI systems can analyze vast amounts of data created by IoT devices to identify patterns that might not be evident and are associated with cyber threats [32].

Corresponding email: nolangael@writesate.edu

AI technologies improve:

- Threat detection
- Behavioral analysis
- Predictive analytics
- Incident response automation
- Malware classification
- Risk prioritization
- Security monitoring

AI-driven security systems operate continuously and adapt dynamically to evolving threats.

**B. MACHINE LEARNING APPLICATIONS**

Machine learning algorithms are widely used in IoT cybersecurity.

**I. Supervised Learning**

Supervised learning models which are trained on labeled data to identify known attacks like malware, spam, phishing, and intrusions.

**II. Unsupervised Learning**

Unsupervised learning can be used to detect anomalies by identifying unusual device behaviors and hidden attack patterns.

**III. Reinforcement Learning**

Adaptive cybersecurity systems can be trained as a part of reinforcement learning and can acquire the best defense strategies through continuous interaction with the IoT environments.

**C. DEEP LEARNING IN IOT SECURITY**

Deep learning technologies improve the detection of sophisticated cyber threats in IoT ecosystems.

Deep learning models are used for:

- Malware detection
- Traffic classification
- Intrusion detection
- Image-based security analysis
- Voice and biometric authentication

Neural network architectures provide improved analytical capabilities for complex IoT environments.

**D. BEHAVIORAL ANALYTICS AND UEBA**

AI-powered User and Entity Behavior Analytics (UEBA) systems monitor user activities, device behavior, network traffic, and access patterns.

Behavioral analytics helps identify:

- Insider threats
- Unauthorized access
- Compromised devices
- Abnormal network activities
- Suspicious login behavior

AI-based behavioral analytics reduces false positives and improves detection accuracy.

**E. NATURAL LANGUAGE PROCESSING IN THREAT INTELLIGENCE**

Natural Language Processing (NLP) enables AI systems to analyze threat intelligence reports, emails, dark web communications, and security logs.

NLP supports:

- Automated phishing detection
- Threat intelligence analysis
- Security reporting
- Chatbot-based support systems
- Incident documentation

**Corresponding email:** nolangael@writesate.edu

## AI-POWERED CYBERSECURITY RISK MANAGEMENT STRATEGIES

### A. INTELLIGENT INTRUSION DETECTION SYSTEMS

In the context of smart IoT environments, AI-based IDS systems will remain vigilant in monitoring network traffic, device behavior, and communication patterns to identify any suspicious activities. AI-driven intrusion detection systems can process enormous amounts of data in real-time and may be better suited to detecting the hidden attack patterns than rule-based detection systems. These systems can contribute to the improvement of the cybersecurity operations by providing better visibility into threats, accuracy in detection, reduction in false positives, and adaptive defense. Machine learning algorithms can power an intelligent IDS system to identify attack patterns that traditional systems are unaware of, as well as suspicious behaviors [33]. As IoT ecosystems continue to expand, an intelligent intrusion detection system becomes more and more imperative to ensure an ongoing state of monitoring and operation security for a level.

### B. PREDICTIVE RISK ANALYTICS

Identifying and controlling vulnerabilities, threats, feeds and device behaviour, predictive analytics can enable organisations to stay ahead of possible cyber attacks. Artificially intelligent predictive cybersecurity solutions can be useful in terms of revealing vulnerable areas and ranking them by threat level to enable organizations to understand where they may be attacked [34]. They can be applied in order to help optimize security resources and in strategic decision making processes and proactive defense planning with the help of predictive analytics. Predictive AI models can be quite useful in enhancing how the organization reacts and adapts to newly detected cyber threats in a smart IoT solution, e.g., where a high volume of real-time data is produced.

### C. AUTOMATED INCIDENT RESPONSE

Attacks are fast, will occur frequently and require quick response, within seconds. Security Orchestration, Automation and Response (SOAR) artificial intelligence (AI) is able to map the plan of action of high-stakes security operations including threat containment, device isolation, malware remediation, alert prioritization and recovery coordination. Incident response systems are crucial in automating the incident response process and streamlining the response timelines to deal with the constraints that are presented by cyber incidents. The systems can also help organizations to stay business continuously and improve their recovery capability in highly dynamic IoT environments. On one hand, automation is capable of enhancing efficiency but in case it involves dealing with the more complex cyber security incidents, it is necessary to include a human element to ensure that everything is in check and that it can be traced.

### D. ZERO TRUST SECURITY MODELS

This is a continuous and constant process that involves users, device, and network activities as it is never trust, always verify with Zero Trust Architecture. Zero Trust systems that are powered by AI offer dynamic access control, perpetual authentication, behavior verification and context-aware authorization. Such ingenious security structures minimize possible vulnerabilities and access to distributed IoT networks. Zero Trust solutions are becoming even more important to ensure the cybersecurity resilience of the numerous ‘smart IoT' devices in the IoT system, which are interconnected and work across cloud-based and edge architectures.

### E. BLOCKCHAIN AND AI INTEGRATION

In addition, Blockchain technology provides additional security benefits for IoT ecosystems, promoting transparency, integrity, and trust. Using blockchain technology alongside AI-powered cybersecurity solutions allows for secure device authentication, decentralized security management, unalterable audit logs, and automated smart contracts. Using blockchain, cybersecurity operations can be performed more reliably, robustly, and securely, protecting data integrity and minimizing the risk of unauthorized data manipulation. Complex distributed IoT systems are now being considered under the combined application of a mix of AI and blockchain designs.

### F. EDGE AND CLOUD SECURITY ARCHITECTURES

Cloud computing and edge computing have become important components in today's IoT ecosystems, particularly in terms of data processing and storage, and intelligent operations. AI-powered edge and cloud security systems provide real-time threat monitoring, distributed security analytics, cloud workload security, API security analytics, and encryption management. The use of Edge AI technologies helps to improve local decision-making processes based on local processing of data near the IoT device to reduce latency and increase the responsiveness of operations. AI security solutions that are cloud-based can provide the scalability and centralized management of threat intelligence to better secure large-scale smart ecosystems.

### I. PREDICTIVE RISK ANALYTICS

Predictive analytics enables organizations to anticipate cybersecurity risks before incidents occur.

**Corresponding email:** nolangael@writesate.edu

AI models analyze:

- Historical attack data
- Vulnerability trends
- Threat intelligence feeds
- Device behaviors
- Environmental conditions

Predictive cybersecurity improves risk prioritization and proactive defense planning.

**II. AUTOMATED INCIDENT RESPONSE**

Modern cyberattacks occur rapidly, making manual response processes insufficient.

AI-powered Security Orchestration, Automation, and Response (SOAR) systems automate:

- Threat containment
- Device isolation
- Alert prioritization
- Malware removal
- Recovery coordination

Automation improves operational efficiency and reduces incident response times.

**III. ZERO TRUST SECURITY MODELS**

Zero Trust Architecture (ZTA) follows the principle of "never trust, always verify."

AI-enhanced Zero Trust systems provide:

- Continuous authentication
- Dynamic access control
- Behavioral verification
- Context-aware authorization
- Risk-based identity management

Zero Trust strategies are particularly important in distributed IoT environments.

**IV. BLOCKCHAIN AND AI INTEGRATION**

Blockchain technologies improve transparency, integrity, and trust within IoT ecosystems.

AI and blockchain integration supports:

- Secure device authentication
- Immutable audit trails
- Decentralized security management
- Smart contract automation
- Data integrity protection

Blockchain enhances the resilience of AI-powered cybersecurity frameworks.

**V. EDGE AND CLOUD SECURITY ARCHITECTURES**

IoT ecosystems increasingly rely on cloud computing and edge computing infrastructures.

AI-powered edge and cloud security systems support:

- Real-time threat monitoring
- Distributed security analytics
- Cloud workload protection
- Data encryption management
- API security analysis

Edge AI reduces latency and improves local decision-making capabilities.

**ORGANIZATIONAL CYBERSECURITY GOVERNANCE IN IOT ECOSYSTEMS**

**A. GOVERNANCE AND LEADERSHIP**

Maintaining a good cybersecurity risk management involves good governance structures of an organization.

Leadership responsibilities include:

**Corresponding email:** nolangael@writesate.edu

- Defining cybersecurity policies
- Allocating resources
- Establishing risk management strategies
- Ensuring regulatory compliance
- Supporting workforce development

The management of cybersecurity must be in balance with company goals and digital transformation plans.

**B. RISK MANAGEMENT FRAMEWORKS**

Enterprise risk management systems should consider AI-enabled cybersecurity as a part of the company.

Risk management activities include:

- Threat modeling
- Vulnerability assessments
- Continuous monitoring
- Risk prioritization
- Business impact analysis

AI improves the speed and accuracy of cybersecurity risk assessments.

**C. WORKFORCE DEVELOPMENT AND SECURITY AWARENESS**

Human error remains a major contributor to cybersecurity incidents.

Organizations should invest in:

- Cybersecurity awareness training
- AI literacy programs
- Incident response exercises
- Phishing simulations
- Cross-functional collaboration

Continuous workforce development strengthens organizational resilience.

**D. REGULATORY COMPLIANCE**

IoT ecosystems must comply with cybersecurity and privacy regulations.

Important frameworks include:

- NIST Cybersecurity Framework
- ISO/IEC 27001
- GDPR
- HIPAA
- PCI DSS
- Cyber Resilience Act

AI-powered systems can support compliance monitoring and automated reporting.

**CHALLENGES AND ETHICAL CONCERNS**

**A. ADVERSARIAL AI ATTACKS**

Adversarial attacks such as manipulated inputs, poisoned training data, and exploitation of models can be directed towards AI systems.

Such attacks may undermine the ability of threat detection and security activities.

**B. PRIVACY AND DATA PROTECTION**

IoT ecosystems collect vast amounts of personal and operational data.

Privacy challenges include:

- Data ownership issues
- Unauthorized surveillance
- Cross-border data transfers
- Consent management
- Sensitive information exposure

**Corresponding email:** nolangael@writesate.edu

Organizations must implement strong privacy governance frameworks.

**C. ALGORITHMIC BIAS AND EXPLAINABILITY**

Biased datasets may produce unfair or inaccurate cybersecurity outcomes.

Explainable AI frameworks are essential for:

- Transparency
- Accountability
- Regulatory compliance
- Ethical governance
- Trust building

**D. WORKFORCE SKILL SHORTAGES**

The shortage of cybersecurity and AI professionals remains a significant challenge.

Organizations require expertise in:

- Machine learning
- Cloud security
- IoT architectures
- Threat intelligence
- Ethical AI governance

**E. ETHICAL GOVERNANCE**

AI-driven cybersecurity raises ethical concerns related to:

- Surveillance practices
- Autonomous decision-making
- Human accountability
- Privacy intrusion
- AI weaponization

Sustainable implementation requires responsible AI governance structures.

**FUTURE TRENDS IN AI-POWERED IOT CYBERSECURITY**

**A. GENERATIVE AI IN CYBERSECURITY**

AI-based technologies aid in automated threat detection, smart assistants, and dynamic cybersecurity systems.

Nevertheless, malware generation, social engineering attacks, and phishing can also be automated with the help of generative AI by cybercriminals.

**B. FEDERATED LEARNING**

Federated learning is a type of training that allows AI models to be trained in a collaborative manner without the centralization of data.

Benefits include:

- Enhanced privacy protection
- Collaborative threat intelligence
- Reduced data exposure
- Improved scalability

**C. EXPLAINABLE AI**

Future cybersecurity systems will increasingly emphasize transparency and interpretability.

Explainable AI improves:

- User trust
- Ethical accountability
- Decision-making clarity
- Compliance management

**D. AUTONOMOUS SECURITY SYSTEMS**

Future IoT ecosystems will rely on autonomous AI-driven security infrastructures capable of:

**Corresponding email:** nolangael@writesate.edu

- Continuous monitoring
- Self-healing mechanisms
- Automated response
- Dynamic adaptation
- Predictive threat management

**E. QUANTUM-RESISTANT CYBERSECURITY**

Quantum computing may disrupt current encryption standards.

Organizations must prepare for:

- Post-quantum cryptography
- Quantum-resistant security protocols
- Advanced threat analysis capabilities

**CONCLUSION**

Smart IoT (Internet of Things) ecosystems are rapidly expanding and have changed the entire landscape of modern digital infrastructures and at the same time created major challenges in cybersecurity. The interconnection of IoT devices and complex environments with cloud systems, edge computing, and various IoT networks exposes these environments to cyberattacks, data breaches, ransomware, insider threats, and AI-powered cyber exploitation.

In the smart IoT context, the traditional approaches to cybersecurity are not suitable because of the dynamical and distributed nature of such systems. AI has thus become a key technology for managing cybersecurity risks. AI-driven solutions enhance threat detection, anomaly analysis, predictive analytics, behaviour monitoring, automated incident response and adaptive defence.

The technologies such as machine learning, deep learning, behavioral analytics, natural language processing, and reinforcement learning empower organizations with intelligent capabilities to secure modern IoT environments. AI-powered cybersecurity solutions ensure the continuity, resilience, and proactive risk management of operations.

However, other issues in the sphere of AI include adversarial attacks, privacy, bias in the algorithm, ethical governance, labor shortage and regulatory compliance. This is an amalgamation of automation and transparency, accountability and human oversight, a huge challenge.

In the future, autonomous security systems, federated learning, explainable AI, blockchain security integration, and quantum-resistant security solutions will be instrumental in the security solutions of the IoT ecosystem. Cyber security risk management tools powered by AI will aid organizations to safeguard their critical infrastructure, facilitate the sustainability of their business processes and jumpstart sustainable cyber security change.

Finally, AI-based cybersecurity risk management is surfacing as an effective strategic resource to the security, resilience and sustainability of smart IoT systems.

**REFERENCES**

[1] J. Bolanos, “A holistic framework for AI-driven cyber risk management in IoT ecosystems,” *Int. J. Artif. Intell. Mach. Learn.*, vol. 4, no. 1, pp. 80–93, 2024.

[2] P. Radanliev, D. De Roure, C. Maple, J. R. Nurse, R. Nicolescu, and U. Ani, “AI security and cyber risk in IoT systems,” *Front. Big Data*, vol. 7, Art. no. 1402745, 2024.

[3] T. Simanjuntak, “Emerging cybersecurity threats in the era of AI and IoT: A risk assessment framework using machine learning for proactive threat mitigation,” *Int. J. Inf. Syst. Innov. Technol.*, vol. 3, no. 1, pp. 15–23, 2024.

[4] A. Adewuyi et al., “The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems,” *convergence*, vol. 20, p. 21, 2024.

[5] M. Kalinin, V. Krundyshev, and P. Zegzhda, “Cybersecurity risk assessment in smart city infrastructures,” *Machines*, vol. 9, no. 4, Art. no. 78, 2021.

[6] U. Imtiaz, “Investigating the impact of phishing attacks on organizational cybersecurity posture,” *Spectrum Eng. Sci.*, pp. 1758–1780, 2025.

[7] S. Butt, “Impact of e-banking service quality on customers’ behavior intentions mediating role of trust,” *Global Manag. J. Acad. Corp. Stud.*, vol. 11, no. 2, pp. 1–21, 2021.

**Corresponding email:** nolangael@writesate.edu

[8] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, M. Flores, and I. Ortiz, "Integration of AI and IoT approaches for evaluating cybersecurity risk on smart city," in *Artificial Intelligence-based Internet of Things Systems*, Cham, Switzerland: Springer, 2022, pp. 305–333.
[9] F. Amin and U. Imtiaz, "Mitigating advanced persistent threats: A framework for enhancing organizational cybersecurity posture," *J. Eng. Comput. Intell. Rev.*, vol. 3, no. 1, pp. 99–113, 2025.
[10] S. M. H. Shah, F. Amin, and A. Khan, "Cyber-resilient mobile edge computing: A deep neural approach for secure and efficient task offloading," *Asian Bull. Big Data Manag.*, vol. 5, no. 1, pp. 200–215, 2025.
[11] S. Butt, I. Mubeen, and A. Ahmed, "Corporate social responsibility and firm financial performance: Moderating role of ethical leadership and social capital," *JISR Manag. Soc. Sci. Econ.*, vol. 20, no. 1, pp. 165–186, 2022.
[12] S. T. Hasan, "Machine learning models for forecasting employee demand in healthcare HR," *J. Eng. Comput. Intell. Rev.*, vol. 3, no. 2, pp. 159–172, 2025.
[13] G. Ali, M. M. Mijwil, B. A. Buruga, M. Abotaleb, and I. Adamopoulos, "A survey on artificial intelligence in cybersecurity for smart agriculture: State-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns," *Mesopotamian J. Comput. Sci.*, vol. 2024, pp. 53–103, 2024.
[14] M. Schmitt, "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection," *J. Ind. Inf. Integr.*, vol. 36, Art. no. 100520, 2023.
[15] S. Islam, N. Basheer, S. Papastergiou, M. Ciampi, and S. Silvestri, "Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure," *J. Reliab. Intell. Environ.*, vol. 11, no. 3, Art. no. 12, 2025.
[16] S. T. Hasan, "Mitigating algorithmic bias in AI-driven hiring systems in the United States," *J. Bus. Insight Innov.*, vol. 5, no. 1, pp. 78–90, 2026.
[17] T. S. AlSalem, M. A. Almaiah, and A. Lutfi, "Cybersecurity risk analysis in the IoT: A systematic review," *Electronics*, vol. 12, no. 18, Art. no. 3958, 2023.
[18] T. Soni, R. Kaur, D. Gupta, A. Sharma, and G. Gupta, "The cybersecurity ecosystem: Challenges, risk and emerging technologies," in *2023 7th Int. Conf. Trends Electron. Inform. (ICOEI)*, Apr. 2023, pp. 699–703.
[19] P. Radanliev, "Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing," *J. Cyber Secur. Technol.*, vol. 9, no. 1, pp. 28–78, 2025.
[20] M. T. Islam, S. Ahmad, M. A. Rahman, and M. A. Rahaman, "Neural network–based risk prediction and simulation framework for medical IoT cybersecurity: An engineering management model for smart hospitals," *Int. J. Sci. Interdiscip. Res.*, vol. 5, no. 2, pp. 30–57, 2024.
[21] R. Bhardwaj, S. Gogula, B. Bhabani, K. Kanagalakshmi, A. Mukherjee, and D. Vetrithangam, "Machine learning and artificial intelligence for detecting cyber security threats in IoT environment," in *Natural Language Processing for Software Engineering*, 2025, pp. 1–14.
[22] A. A. M. Jabir and F. Jahan, "High entropy alloy at high temperature and pressure," *Int. J. Adv. Eng. Technol.*, vol. 16, no. 6, pp. 500–517, 2023.
[23] M. T. Islam, A. Azeem, M. Jabir, A. Paul, and S. K. Paul, "An inventory model for a three-stage supply chain with random capacities considering disruptions and supplier reliability," *Ann. Oper. Res.*, vol. 315, no. 2, pp. 1703–1728, 2022.
[24] F. T. Zohora and P. Paul, "Maternocare prediction for maternal and child well-being using survey data and machine learning approaches," *Excel Int. J. Technol. Eng. Manag.*, vol. 11, no. 4, pp. 170–180, 2024.
[25] M. S. R. Aronno et al., "A study of cyber bullying classification using social media and textual analysis based on machine learning approaches," in *2023 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2023, pp. 1–8.
[26] M. Farooq and M. H. Khan, "Artificial intelligence-based approach on cybersecurity challenges and opportunities in the Internet of Things & edge computing devices," *Int. J. Eng. Comput. Sci.*, vol. 12, no. 7, pp. 25763–25768, 2023.
[27] A. Rahman and S. S., "National Economic Impact Measurement of Cybersecurity Failures in US Financial Technology Platforms," *International Journal of AI, Engineering and Management Studies (IJAIEMS)*, pp. 17–38, 2025.

**Corresponding email:** nolangael@writesate.edu

[28] S. Sultana and A. Rahman, "Deep Learning-Based Phishing Website Detection: Integrating Visual Design Analysis with URL Feature Extraction," *World Wide Journal of Multidisciplinary Research and Development*, vol. 11, no. 12, pp. 25–29, Dec. 2025.
[29] T. James, "A Review of Blockchain-Integrated Enterprise Systems for Secure Operations, Economic Resilience, and Industry Transformation," *Journal of Computational Systems & Engineering Insights*, vol. 1, no. 1, 2023.
[30] A. Hossein, "Enhancing Business Performance Through Artificial Intelligence and Analytics: Evidence from US Organizations," *Journal of Computational Systems & Engineering Insights*, vol. 2, no. 1, pp. 1–10, 2024.
[31] M. S. Islam and T. A. Shiva, "Virtual Cognitive Behavioural Therapy in Rural US Communities: Effectiveness and Reach," *Journal of Business Insight and Innovation*, vol. 3, no. 2, pp. 60–76, 2024.
[32] T. A. Shiva, J. G. Brown, A. A. McField, R. E. Osborne, and C. D. Oberle, "Cultural Associations with Prosocial Behaviors and Attitudes Among Asian Americans," *Asian American Journal of Psychology*, vol. 16, no. 3, pp. 268–278, 2025, doi: 10.1037/aap0000368.
[33] U. Twaha, A. Mosaddeque, and M. Rowshon, "Accounting Implications of Using AI to Enhance Incentives for Wireless Energy Transmission in Smart Cities," *International Journal of Management Research and Global Education*, vol. 6, no. 2, pp. 1208–1218, 2025.
[34] U. Twaha and Y. Arfin, "An AI-Driven Framework for Real-Time Fake News Detection: Developing a Machine Learning-Based Filter for News Platforms in the United States," *International Journal of Future Engineering Innovations (IJFEI)*, vol. 2, no. 4, pp. 158–169, 2025, doi: 10.54660/IJFEI.2025.2.4.158-169.

**Corresponding email:** nolangael@writesate.edu