STM JOURNALS

International Journal of
Wireless Security and Networks

ISSN: 2584-0703
Volume 4, Issue 1, 2026
January–April
DOI (Journal): 10.37591/IJWSN

https://journals.stmjournals.com/ijwsn

Review IJWSN

Hybrid Intelligence in Cyber Security: A Study

Kazi Kutubuddin Sayyad Liyakat*

Abstract

The digital landscape is a battlefield of escalating complexity, where the volume, velocity, and sophistication of cyber threats have exponentially outpaced human-centric defense models. Traditional rule-based security systems and siloed artificial intelligence (AI) solutions, while valuable, are increasingly brittle, overwhelmed by zero-day exploits, polymorphic malware, and coordinated, state-sponsored campaigns that operate in the shadows of big data. This paper posits that the paradigm of cybersecurity must fundamentally shift from one of automated reaction to one of cognizant anticipation. We introduce and explore the framework of hybrid intelligence (HI) as the cornerstone of next-generation cyber defense. HI is not merely a tool but a synergistic partnership, a fusion of the computational prowess and pattern recognition capabilities of AI with the nuanced understanding, ethical reasoning, and creative problem solving of human intelligence. This abstract outline a future where AI algorithms, trained on global threat telemetry, perform lightning-fast triage and anomaly detection at a scale impossible for humans, while human analysts are elevated to strategic overseers: interpreting context, managing escalation, and authorizing nuanced responses. It is within this collaborative loop, machine speed with human wisdom, that we can construct a cyber-immune system: adaptive, resilient, and inherently intelligent.

Keywords: Hybrid intelligence, cybersecurity, artificial intelligence, human intelligence, threat detection

INTRODUCTION

A digital battlefield rages a maelstrom of unseen threats and silent skirmishes. Every click, every download, and every interconnected device is a potential vector for an enemy that is increasingly sophisticated, fast, and relentless. In this constant war, traditional defenses, whether purely human or purely machine, began to show their cracks. Human analysts are overwhelmed by the sheer volume of data, suffering from alert fatigue and an inability to spot the needle in a haystack across petabytes of traffic. AI, while brilliant at pattern recognition and speed, often lacks intuition, contextual understanding, and ethical judgment to truly outmaneuver a creative, malicious human actor [1–3].

Enter Hybrid Intelligence

The strategic, symbiotic fusion of human intelligence (HI) and artificial intelligence (AI) to create a cybersecurity force greater than the sum of its components. This is not just AI assisting humans, nor humans simply overseeing AI; it is a true collaboration, a dynamic feedback loop where each augment informs and elevates the other.

***Author for Correspondence**
Kazi Kutubuddin Sayyad Liyakat
E-mail: drkkazi@gmail.com

Professor and Head, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

Received Date: September 09, 2025
Accepted Date: September 10, 2025
Published Date: February 24, 2026

Citation: Kazi Kutubuddin Sayyad Liyakat. Hybrid Intelligence in Cyber Security: A Study. International Journal of Wireless Security and Networks. 2026; 4(1): 1–9p.

Imagine the cybersecurity operations center of tomorrow. AI acts as an omnipresent sentinel, tireless data miner, and predictive analyst. It sifts through astronomical datasets in real time, identifying anomalies, correlating seemingly disparate events, and detecting subtle behavioral shifts that might indicate an attack. It automates routine responses, instantly blocks known threats,

and flags high-priority incidents for human intervention. AI is not just an alert system; it is an intelligent filter and a threat intelligence hub that learns and adapts at machine speed [4–7].

However, when a truly novel attack surfaces, a zero-day exploit, sophisticated social engineering campaign, or highly targeted advanced persistent threat, pure AI falters. This is where human intelligence shines. The seasoned cybersecurity analyst, powered by years of experience, intuition, and a profound understanding of human psychology, takes steps [8]. They provide a crucial context, asking "why?" beyond the "what?" they see. They can analyze the attacker's intent, devise creative counterstrategies, negotiate complex geopolitical landscapes, and make critical ethical decisions that no algorithm can replicate [9].

The beauty of HI lies in this iterative dance:

- *AI identifies*: Pinpoints suspicious activity across vast networks, far beyond human capacity.
- *Humans investigate*: Adds context, intuition, and strategic thinking to determine if an anomaly is a genuine, novel threat, or false positive.
- *Humans train AI*: Feeds newly identified threats, successful countermeasures, and contextual understanding back into learning models of AI, making it smarter and more resilient.
- *AI empowers humans*: Provides analysts with distilled, prioritized information, frees them from mundane tasks, and allows them to focus on high-level strategic defense and creative problem solving.

This synergistic ballet creates an unparalleled defense mechanism. This implies faster detection, fewer false positives, more intelligent and adaptive responses, and a significant reduction in the cognitive load on human analysts. It transforms the cybersecurity team from reactive responders into proactive hunters, always learning and constantly evolving [10].

The centaur metaphor, often used in chess where a human-computer team can outperform either a human grandmaster or a supercomputer alone, is profoundly apt for cybersecurity. Humans provide a strategic vision, adaptability, and an ethical bedrock. The machine provides processing power, scale, and speed. Together, they create formidable guardians for the digital world [11].

The future of cybersecurity is not about replacing humans with machines nor about machines simply serving humans. It is a profound, integrated partnership where the unique strengths of human ingenuity and AI converge. HI is not just a technological advancement; it is a philosophical shift, forging a resilient, intelligent, and truly adaptive defense against an endless storm of cyber threats. It is the ultimate digital guardian, an evolving learning organism capable of protecting the fabric of interconnected lives [12].

FRAMEWORK FOR CYBERSECURITY POWERED BY HYBRID INTELLIGENCE

The digital battleground is ceaseless, its adversaries ever-morphing chimeras, and the volume of data is overwhelming. In this high-stakes environment, traditional reliance on human analysts, though brilliant, struggles against the sheer scale and speed of modern threats. Conversely, the notion of a fully autonomous AI defense, while alluring, falls short in its inability to grasp nuanced contexts, ethical dilemmas, and the creative intent behind novel attacks. Therefore, the future of cybersecurity lies not in a binary choice, but in a symbiotic fusion: hybrid intelligence.

A framework for cybersecurity using HI is not merely about AI assisting humans or humans overseeing AI. It is a collective cognitive system where the strengths of AI and human intelligence (HI) are seamlessly interwoven, creating a defense mechanism that is more resilient, adaptive, and proactive than either could be alone.

This framework is built on three foundational pillars, each demanding a continuous, iterative loop of human-AI collaboration.

Pillar 1: Augmented Threat Detection and Predictive Analytics

Challenge

Identifying subtle anomalies amidst petabytes of legitimate traffic, recognizing zero-day exploits, and predicting future attack vectors.

The Hybrid Approach

Role of AI

- *Rapid data ingestion and anomaly detection*: Machine Learning algorithms constantly analyze network traffic, log data, endpoint telemetry, and user behavior for deviations from the established baselines. They can pinpoint minute changes, unusual access patterns, or sudden spikes in activity far faster and on a greater scale than humans.
- *Threat intelligence correlation*: AI systems aggregate and correlate vast amounts of global threat intelligence, identifying known malware signatures, Internet Protocol (IP) addresses associated with malicious activity, and emerging attack campaigns in real time.
- *Predictive modeling*: Deep learning models trained on historical breach data and threat actor tactics can forecast potential attack vectors and vulnerable points, moving defense from reactive to proactive.

Role of Human Intelligence

- *Contextualization and false positive reduction*: Security analysts review AI-generated alerts, providing the critical human context necessary to differentiate between genuine threats and benign anomalies. They fine-tuned AI models by marking false positives and teaching the system what truly matters.
- *Intuitive threat hunting*: Armed with initial insights of AI, human threat hunters can then delve deeper, using their intuition and understanding of attacker psychology to connect seemingly disparate alerts, uncover sophisticated, multi-stage attacks, and identify novel threats on which AI has not yet been trained.
- *Strategic risk assessment*: Humans translate technical findings of AI into business risk, prioritizing vulnerabilities and potential impacts based on organizational values and real-world implications.

Loop

AI flags, humans contextualize and refine, and AI learns and improves its flagging based on human feedback, leading to more accurate predictions and fewer false alarms.

Pillar 2: Intelligent Incident Response and Remediation

Challenge

Containing breaches quickly, accurately, and with minimal operational disruption, while also understanding the attacker's intent and impact.

The Hybrid Approach

Role of AI

- *Automated containment and prioritization*: Security orchestration, automation, and response (SOAR) platforms powered by AI can automatically isolate infected endpoints, block malicious IPs, and revoke compromised credentials based on predefined playbooks. They prioritize incidents based on severity and potential impact and route critical alerts to human experts.
- *Forensic data collection and synthesis*: AI agents can rapidly gather and organize relevant forensic data (logs, memory dumps, and network captures) from compromised systems, presenting them in an easily digestible format for human analysis.

- *Rapid remediation suggestions*: Based on the identified threats, AI can suggest immediate remediation steps, such as patching vulnerabilities, updating firewall rules, or deploying specific security configurations.

Role of Human Intelligence

- *Strategic decision-making and override*: While AI can execute automated responses, humans make critical strategic decisions: when to override an automated action (e.g., to preserve evidence), when to involve legal or Public Relations (PR), and how to manage the broader organizational response.
- *Deep forensic analysis and root cause identification*: Human experts perform in-depth forensic analysis, going beyond the AI's initial data correlation to understand how and why of an attack, identify the root cause, and formulate long-term preventative measures.
- *Ethical and contextual judgment*: Humans assess the ethical implications of response actions, ensuring that automated responses do not inadvertently harm legitimate users or critical business processes. They also communicate with stakeholders.

Loop

AI executes initial containment and gathers data, humans analyze and make strategic decisions, AI updates its playbooks and response protocols based on human-approved actions and makes future responses smarter.

Pillar 3: Adaptive Defense and Continuous Learning

Challenge

Keeping pace with the ever-evolving threat landscape, learning from past incidents, and proactively strengthening defenses.

The Hybrid Approach

Role of AI

- *Vulnerability management and patch prioritization*: AI continuously scans for vulnerabilities, correlates them with threat intelligence, and prioritizes patching based on the potential exploitability and asset criticality.
- *Automated policy optimization*: AI can analyze the effectiveness of existing security policies and suggest modifications to improve their efficacy without hindering legitimate operations.
- *Adversarial AI countermeasures*: AI systems can be trained to recognize and defend against AI-driven attacks such as deepfakes used in social engineering or AI-generated malware variants.

Role of Human Intelligence

- *Security architecture and policy design*: Humans are responsible for overarching security architecture, designing new defense mechanisms, and defining high-level security policies that AI systems then help implement and optimize.
- *Red teaming and scenario planning*: Human "attackers" actively test the hybrid defense system, creating novel attack scenarios (including those designed to bypass AI) to identify weaknesses and train AI on new threat patterns.
- *Ethical AI governance and explainable AI (XAI):* Humans guide the ethical development and deployment of AI to ensure transparency. XAI allows humans to understand the reasoning behind AI's decisions, foster trust, and enable continuous improvement of models and the logic of AI.

Loop

Humans design and test, AI optimizes and learns, humans review and refine suggestions of AI, collectively enhancing the entire security posture.

Key Enablers of the Framework

- *Seamless human-AI interfaces*: intuitive dashboards, natural language processing for querying AI, and visualization tools that understandably present complex data.

- *Explainable AI (XAI):* The ability of AI to articulate reasoning, foster trust, and allow humans to confirm decisions and identify biases.
- *Continuous learning pipelines*: Mechanisms for AI models to be constantly updated with new data, human feedback, and threat intelligence.
- *Skills transformation*: Training security professionals to effectively collaborate with AI, understand its capabilities and limitations, and leverage its power.
- *Data quality and governance*: Robust collection, curation, and secure management of high-quality data to fuel AI learning.

The HI framework transforms cybersecurity from a Sisyphean task to an adaptive, intelligent ecosystem. It liberates human experts from the drudgery of data overload and repetitive tasks, allowing them to focus on strategic thinking, creative problem solving, and the unique human aspects of threat understanding. Concurrently, it imbues AI with the crucial context, ethical judgment, and adaptability that only human intellect can provide.

By embracing this collective cognitive approach, organizations can build a "Hybrid Sentinel" – a robust, intelligent, and continuous learning defense that not only detects and responds to known threats with unparalleled speed and scale, but also anticipates, adapts to, and neutralizes the unknown with the ingenuity and wisdom of its combined intelligence. The future of cybersecurity is neither artificial nor merely human; it is the powerful synergy of both, working in concert to safeguard our digital world.

EVALUATION CRITERIA FOR CYBERSECURITY USING HYBRID INTELLIGENCE: A NEXT-GEN APPROACH

In the rapidly evolving cybersecurity landscape, traditional methods alone often fall short of sophisticated and adaptive cyber threats. HI, which is an intelligent fusion of human expertise and AI, has emerged as a powerful paradigm for enhancing detection, response, and resilience. However, integrating human judgment with machine learning (ML) and automated systems requires well-defined evaluation criteria to ensure efficiency, accuracy, and adaptability.

Threat Detection Accuracy (Precision and Recall)

A core metric in cybersecurity is the ability to correctly identify threats without excessive false positives or false negatives. HI must be evaluated based on the following:

- *AI detection performance*: How accurately do ML models flag anomalies?
- *Human validation accuracy*: Do security analysts effectively confirm or refine the AI-generated alerts?
- *Adversarial robustness*: Can the system resist evasion techniques like adversarial attacks?

Response Time and Decision Efficiency

Cyber threats demand real-time mitigation. HI should be assessed on:

- *Automation speed:* How quickly does AI triage incidents?
- *Human-AI collaboration latency*: How seamlessly do analysts interact with AI recommendations?
- *Incident resolution time*: Does the combined approach reduce the mean time to detect (MTTD) and respond (MTTR)?

Adaptability and Continuous Learning

Static solutions fail to respond to dynamic threats. A robust HI system can be determined as follows:

- *Self-learning capability*: Can AI models evolve with new threat intelligence?
- *Human feedback integration*: Does analyst input improve AI decision-making over time?
- *Threat anticipation*: Does the system proactively predict novel attack vectors?

Scalability and Operational Efficiency

Cybersecurity solutions must handle increasing data volumes without degrading performance:

- *Resource optimization*: Does HI balance human workload and AI processing?
- *Deployment flexibility*: Can it operate across clouds, premises, and hybrid environments?
- *Cost-effectiveness*: Does automation reduce manual overhead without sacrificing security?

Explainability and Trustworthiness

For human analysts to trust AI, the system must be transparent:

- *Interpretability*: Are AI-driven decisions explainable in human-understandable terms?
- *Bias and fairness*: Are AI models free from biases that could lead to flawed judgments?
- *Human oversight*: Can experts override AI decisions when necessary?

Compliance and Ethical Considerations

Hybrid systems must align with regulations and ethical norms:

- *Regulatory alignment*: Does it comply with GDPR, NIST, or other cybersecurity frameworks?
- *Ethical AI use*: Are privacy and ethical boundaries respected in decision-making?

HI represents the future of cybersecurity by blending AI speed with human intuition. By evaluating systems based on accuracy, speed, adaptability, scalability, transparency, and compliance, organizations can build resilient defenses. As cyber threats grow in complexity, the synergy between humans and machines will define the next era of digital protection.

RESULTS AND DISCUSSION ON HYBRID INTELLIGENCE IN CYBERSECURITY

The digital frontier is a perpetual battleground that constantly shifts with new threats, zero-day exploits, and increasingly sophisticated adversaries. Traditional cybersecurity, whether purely human-driven or solely reliant on autonomous AI, often finds itself playing a catch-up role. Human analysts are overwhelmed by alert fatigue, while AI, for all its speed, can lack nuanced understanding, creativity, and ethical judgment of human intelligence. This is where hybrid intelligence—the seamless fusion of human cognition with artificial intelligence—emerges not just as an evolution but as the inevitable future of our digital defense.

The expected results of deploying HI in cybersecurity are transformative and usher in an era of unprecedented vigilance, adaptability, and resilience.

Amplified Detection and Precision: Beyond the Noise

One of the immediate and profound impacts of HI is the dramatic improvement in threat detection. Unparalleled ability of AI to process vast datasets, identify subtle anomalies, and correlate seemingly unrelated events at machine speed will be augmented by human intuition and contextual understanding.

- *Result*: A significant reduction in false positives allowed security teams to focus on genuine threats. AI will flag potential indicators, while human analysts, armed with experience and a broader understanding of business operations and geopolitical contexts, will rapidly validate or dismiss alerts. This synergy means fewer missed attacks (AI breadth) and less effort wasted (human precision).
- *Example:* An AI may detect unusual data transfer patterns. A human analyst, knowing a specific department only onboarded a new cloud service, can discern whether it is a legitimate activity or a potential exfiltration attempt, teaching AI in the process.

Accelerated and Informed Incident Response: From Reactive to Proactive

Incident response is currently a race against time, often hindered by the sheer volume of data and the complexity of attack chains. The HI promises to compress response times from hours or days to minutes, fundamentally altering the attacker's advantage.

- *Result*: Automated initial containment and remediation (AI), followed by strategic context-aware decision-making (human). AI can rapidly isolate infected systems, block malicious IPs, and deploy patches, whereas human experts focus on understanding the attacker's motive, preventing recurrence, and navigating the legal and reputational fallout.
- *Example*: Upon detecting ransomware, AI automatically quarantines affected endpoints and rolls back to a last-known good state. Simultaneously, it presents the human team with root cause analysis, threat intelligence, and recommended strategic counter-offensives, empowering them to make high-level decisions swiftly.

Proactive Threat Hunting and Predictive Analytics: Anticipating the Unseen

Shifting from a reactive "whack-a-mole" approach to a proactive predictive posture is a holy grail in cybersecurity. HI makes this reality.

- *Result*: The ability to anticipate attacks and build defenses before they materialize. AI can sift through global threat intelligence, dark web chatter, and internal telemetry to identify nascent attack campaigns or tactics, techniques, and procedures (TTPs). Human threat hunters leverage these AI-generated insights to formulate hypotheses, conduct deep dives, and actively search for stealthy threats within their networks.
- *Example*: AI may identify a new, unpatched vulnerability affecting critical software alongside a spike in specific credential-stuffing attempts globally. It alerts human hunters to proactively scan their network for indicators of compromise related to this vulnerability or even develop temporary virtual patches before an exploit is widely weaponized.

Adaptability and Resilience Against Zero-Days and Novel Threats

Zero-day exploits and polymorphic malware are a type of traditional security. They bypass known signatures and defy static rules. HI offers a dynamic and evolving defense mechanism.

- *Result*: A continuous learning loop allows defenses to adapt to the speed of the threat. AI continuously learns from new attack patterns, human feedback, and evolving data sets. When a novel threat emerges, the human analyst's creativity and problem-solving skills, augmented by AI's rapid analysis of the characteristics of the new threat, can formulate countermeasures far quicker than isolated systems.
- *Example*: When faced with a never-before-seen malware variant, AI analyzes its behavioral patterns and flags anomalies. The human expert understands the intent behind the behavior, guides the AI on which features to prioritize, and collaboratively develops a new detection signature or behavioral rule from which both systems can disseminate and learn.

Bridging the Skill Gap and Reducing Analyst Burnout

The cybersecurity industry faces severe skill shortages and high burnout rates among security professionals. HI offers a pathway to sustainable talent management.

- *Result*: Empowered, less burdened security workforce. AI will automate mundane, repetitive tasks and free human analysts to focus on complex, strategic, and creative problem solving. This will augment less experienced analysts and effectively democratize expertise by providing them with AI-driven insights and playbooks.
- *Example*: Junior analysts, typically overwhelmed by thousands of daily alerts, can now rely on AI to triage and contextualize the vast majority. They focus their energy on a handful of high-fidelity, complex cases elevated by AI, learning, and gaining experience much faster under the guidance of the system.

HI is not merely a technological upgrade; it is also a paradigm shift in cybersecurity. It promises to elevate defenses from a reactive, signature-based struggle to a proactive, adaptive, and truly intelligent system. By harnessing the strengths of both human ingenuity and AI in a symbiotic relationship, we can expect to build a digital shield that is not only robust but also capable of evolving with the threat

landscape, safeguarding our digital future with unprecedented efficacy and resilience. The era of the "sentient" cyber defense is upon us, and its results will be nothing short of revolutionary.

CONCLUSION

The journey through the realms of cybersecurity reveals a stark truth: Our enemies are agile, adaptive, and increasingly automated. To withstand this tide, defenses cannot be static. The conclusion of this exploration is not the discovery of a silver bullet but the blueprint for a new kind of sentinel—one born from the synergy of humans and machines.

HI is the solution to the limitations of a purely algorithmic approach. AI, for all its powers, lacks context. It can identify a deviation from the norm but cannot discern a clumsy intern from a sophisticated intruder mimicking one. It can execute a pre-programmed containment script but cannot weigh the political fallout of taking a nation-state server offline. Humanity provides consciousness, intuition, and strategic oversight. We are the sages who ask "why," not just.

Conversely, human teams, regardless of their skills, are fundamentally limited by bandwidth and fatigue. We cannot parse terabytes of logs in milliseconds or maintain perfect vigilance across a global network 24/7. AI serves as the indefatigable sentinel, processing the endless noise to present the human expert with a curated set of genuine signals—the proverbial needle in a haystack, already isolated, and held up for inspection.

Therefore, the future of cybersecurity is not a choice between human and AI, but a deliberate and intelligent combination of both. It is a future where:

- *AI handles predictable volume*; humans handle the unpredictable exceptions.
- *AI provides diagnostic metrics*; humans provide diagnostic wisdom.
- *AI executes the response;* humans dictate the rules of engagement.

The implementation of HI is the most pragmatic path forward. It promises a defense that is not only faster and more comprehensive, but also wiser and more ethically grounded. This moves us from a state of constant reaction to empowered resilience. By embracing this partnership, we cease to be mere defenders of digital walls and become architects of a trustworthy digital ecosystem. The sentinel and sage, working as one, can finally secure a future that is not only connected but also safe.

REFERENCES

1. Sauer CR, Burggräf P. Hybrid intelligence – systematic approach and framework to determine the level of human-AI collaboration for production management use cases. Prod Eng. 2025;19(3):525–541. doi:10.1007/s11740-024-01326-7.
2. Jayalath H, Yassin G, Ramaswamy L, Li S. Continual optimization of in-production machine learning systems through semantic analysis of user feedback. In: Rocha AP, Steels L, van den Herik J, editors. Proceedings of the 15th International Conference on Agents and Artificial Intelligence (ICAART); 2023 Feb 22–24; Lisbon, Portugal. Setúbal (Portugal): Science and Technology Publications, Lda (SCITEPRESS); 2023. p. 285–292. doi:10.5220/0011660300003393.
3. Forest JJ. Management discipline: defining a process safety strategy. Process Saf Prog. 2014;33:162–165. doi:10.1002/prs.11642.
4. Burger M, Nitsche AM, Arlinghaus J. Hybrid intelligence in procurement: disillusionment with AI's superiority? Comput Ind. 2023;150:103946. doi:10.1016/j.compind.2023.103946.
5. Liyakat KKS. Machine learning approach using artificial neural networks to detect malicious nodes in IoT networks. In: Udgata SK, Sethi S, Gao XZ, editors. Intelligent systems. Proceedings of the 3rd International Conference on Machine Learning, IoT and Big Data (ICMIB 2023). Lecture Notes in Networks and Systems. Singapore: Springer Nature Singapore; 2024.
6. Jarrahi MH, Lutz C, Newlands G. Artificial intelligence, human intelligence and hybrid intelligence based on mutual augmentation. Big Data Soc. 2022;9. doi:10.1177/20539517221142824.

7. Liu Y, Fu Z. Hybrid intelligence: design for sustainable multiverse via integrative cognitive creation model through human–computer collaboration. Appl Sci. 2024;14(11):4662. doi:10.3390/app14114662.
8. Kazi KSL. KK approach to increase resilience in Internet of Things: a T-cell security concept. In: Darwish D, Charan K, editors. Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions. Hershey (PA): IGI Global Scientific Publishing; 2025. p. 87–120. doi:10.4018/979-8-3693-9491-5.ch005.
9. Abdelghani W, Zayani CA, Amous I, Sèdes F. Trust evaluation model for attack detection in social Internet of Things. In: Proceedings of the 13th International Conference on Risks and Security of Internet and Systems (CRiSIS); 2018 Oct; Arcachon, France. Cham: Springer; 2018. p. 48–64. doi:10.1007/978-3-030-12143-3_5.
10. Mehta M, Patel KA. Enhancing IoT security: a machine learning approach to predicting anomalies in network traffic. In: Manoharan S, Tugui A, Perikos I, editors. Proceedings of the 5th International Conference on Artificial Intelligence and Smart Energy (ICAIS 2025). Information Systems Engineering and Management. Volume 42. Cham: Springer; 2025. p. 279–290. doi:10.1007/978-3-031-90482-0_22.
11. Hodo E, Bellekens X, Hamilton A, Dubouilh PL, Iorkyase E, Tachtatzis C, Atkinson R. Threat analysis of IoT networks using artificial neural network intrusion detection system. 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, Tunisia. 2016. p. 1–6. doi:10.1109/ISNCC.2016.7746067.
12. Khatun MA, Chowdhury N, Uddin MN. Malicious nodes detection based on artificial neural network in IoT environments. 2019 22nd International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh. 2019. p. 1–6. doi:10.1109/ICCIT48885.2019.9038563.

