BOHR International Journal of Internet of things,
Artificial Intelligence and Machine Learning
2026, Vol. 5, No. 1, pp. 1–5
DOI: 10.54646/bijiam.2026.33
www.bohrpub.com

REVIEW

# Generative AI and IoT security: opportunities and challenges

**S. L. Fathima Ruksana**[*†]

Department of Information Technology, Advanced Technological Institute, Sammanthurai, Sri Lanka

[*]**Correspondence:**
S. L. Fathima Ruksana,
fathimaruksanasl@gmail.com

[†]**ORCID:**
S. L. Fathima Ruksana
0009-0003-6956-973X

**Received:** 12 December 2025; **Accepted:** 28 February 2026; **Published:** 02 April 2026

Generative artificial intelligence is one of the frameworks that help to make safe and rational decisions and analyze complex information to foresee risky behaviors. Now the internet of things (IoT) has spread all over the world, and cyberattacks are used to ensure real-time integration of huge amounts of data. But coordinating with threats and attacks, as well as dealing with hackers and using networks, is an important challenge for the security of the classic IoT. Some of them include rule-based detection, rule-based intrusion detection, and signature-based intrusion detection. There are countless possibilities for generative AI (Gen AI), such as advanced anomaly detection, realistic attack simulation, production of artificially generated data to facilitate the prediction of writers, and automated incident management. Besides, there are a few challenges with Gen AI integration to IoT applications. Problems with competitive management, the computing and technological constraints of IoT devices, ethics issues, and numerous ways for hackers to extract false information from sensors using Gen AI are major challenges. In addition, it could be held responsible for publicizing sensitive information from fake datasets and could have problems with the privacy of sensitive data being trained with Gen AI. The main objective of this research work is to do a detailed analysis of IoT security Gen AI technology. The information, in this report for the 2018–2025 periods, was obtained from the current literature. The paper discusses and addresses some key concepts, and based on that, there are opportunities, challenges, and innovative approaches that are crucial for Gen AI utilization. The next generation thinks that Gen AI will be one of the most important technologies that will affect the next generation of IoT cybersecurity solutions. It is important for them to thoroughly analyze the advantages and disadvantages of this technology.

**Keywords:** generative AI, internet of things (IoT), cybersecurity, adversarial attacks, deep learning, edge computing, secure IoT system

## Introduction

Smart cities across the globe have a technological ecosystem that is linked to Internet of Things technology (IoT), and they believe that there are billions of devices connected in business, homes, healthcare, agriculture, and transportation. Based on the projection, more than 15 billion IoT devices have been installed worldwide in 2023, eventually representing more than 25 billion IoT devices deployable in the whole world in 2030 (1). All of these equipment's are important in data collection, analysis, and data transmission, which will aid in the ongoing technological development and optimum decision-making process. With various kinds of devices, there is also the potential of cybersecurity risk, absence of security measures, outdated device firmware, and potentially large-scale scanning from outsiders (2). Additionally, the hackers are getting even higher stakes every single day, making it impossible to protect IoT networks like

that with conventional strategies. Also, some of the advanced attackers and bad guys are not detected at runtime using static rule-based detection.

Models of this type include propagation theories, models based on transformer-based layouts, models based on generative adversarial networks (GANs), and models based on variational autonomous coders (VAEs): generative AI (Gen AI). These models have the ability to train multiple distributions and learn a large amount of probable abstractions and even produce new samples of the data (3, 4). Such built-in capabilities render Gen AI valuable to address the dynamic and unpredictable nature of cyberattacks lurking over IoT. Apart from that, there are a few reasons why such research needs to be performed, as the hacker has high skills and is breaking the protection. This can be explained in international literature with different mitigation measures and be emphasized in the neighborhood studies with the national security protocol.

In doing that; it has classified the analysis of Gen AI security and IoT security and provides a large number of solutions to the majority of the academic criteria. As the IoT industry has grown, it has the possibility to expand to 25 billion devices in the future.. Traditional means of providing security have failed to keep up with the massive number of hackers and their activities. From 2018, there are plenty of authors who have done a lot of reviews utilizing different technologies around the world till 2025, such as GANs and transformers. According to the Sri Lanka study, there is a need for developing localized protocol due to the underdeveloped nature and less citations in the country. This work helps to pinpoint the main difficulties primarily facing Gen AI models with the same constraints of computing power the IoT hardware has to deal with and the fact that the data sets may be poisoned and leaks users' private data and proposes solutions to overcome them. The main objective of this paper is to examine Gen AI with regard to IoT security. Plus, it will alert to problems and future research trends in the latest areas of academic and applied research.

## Literature review

### *IoT security landscape*

The IoT ecosystem is comprised of sensors, actuators, gateways, and cloud platforms. An IoT system typically includes some sensors to gather the data, some actuators to execute the act, some gateways to connect them, and some storage in the cloud to store the data and process the information (5). Also, some IoT devices at this point may be lax in security and could be compromised and accessed by hackers. Certain IoT devices also carry a number of risks that could result in serious hacking and crimes. More than 100,000 devices such as routers and webcams are infected by the Mirai bot network, for instance. Although this attack pointed to the dangers of using fake, unprotected IoT devices, there are lots of resources and applications online so far (2).

The IoT issues include that almost every IoT gadgets needs cloud services. Hackers can steal and take control of the device, and if insecure application programming interfaces (APIs) are used to connect the device to applications of the attackers. In addition, there is the potential for using IoT devices that have weak encryption, meaning that information transferred can be easily deciphered by recipients. Also, since the IoT devices are physically utilized, hackers can easily access them and make changes as per their will. Also, there is the possibility of a man-in-the-middle attack between the device and the server used where data can be stolen. One of the issues is related to privacy, since at times people's profiles or data can be easily retrieved from the IoT devices.

This is where Gen AI comes into the picture when it comes to cybersecurity.

This makes Gen AI highly versatile for modeling very complex behavioral patterns, which has found widespread use in cybersecurity (3), where it can generate realistic synthetic data. For example, GANs have been successfully applied for the development of malware (6), traffic modeling or intrusion detection. As a result of their ability to learn low-dimensional representations of normal behaviors, VAEs have been applied as the tool for anomaly detection (4).

Recently, transformer models are widely adopted in the cybersecurity field for automated incident response, threat detection, and large-scale log analysis (7, 8). They can find the complicated relationships of temporal IoT data with their self-attention mechanism.

### *Securing IoT using the might of generative AI (Gen AI)*

Gen AI integration with IoT security is still in its infancy but is growing quickly. Recent research (9) has demonstrated interest in hybrid IoT, which involves distributed security with the concepts of edge computing, federated learning, and Gen AI. Synthetic IoT traffic can be generated, anomalies can be detected, complex attack scenarios can be simulated, and device behavior can be simulated on Gen AI, which makes it an appropriate platform for next-generation IoT security solutions (10).

## Methodology

A qualified, comprehensive review process is used on this work. From 2018 to 2025, research articles were screened based on predetermined criteria for review. The databases used are Google Scholar, Elsevier ScienceDirect, SpringerLink, the IEEE Digital Library, and the ACM Digital Library.

## Inclusion criteria

- A series of peer-reviewed research has been conducted on cybersecurity challenges of IoT (2).
- Research where a Gen AI model is proposed or tested (3, 11).
- Intrusion detection systems (IDS) (6) experiments:
- Gen AI or IoT-relevant surveys/meta-analyses (12)
- Adversarial/-Ethical Issues consequences research (13)

## Exclusion criteria

- Commercial articles, marketing reports – informal blogs
- If not fundamental, before 2018 (outdated research)
- Articles that do not make any conceptual or experimental contribution

## Data extraction

These have been used in the process of each selected study:

- The kind of Gen AI model employed
- Productivity boosted by eliminating IoT security problems

Identifies important characteristics of the data set.

- Model output and model evaluation data were generated and provided.
- Determined restrictions

This enabled comprehensive knowledge to be developed about the area under investigation. We have adopted a systematic approach for the qualitative review in this paper and integrated the Gen AI in the IoT security domain. This method is planned based on the current research: the five main academic databases to be entered for searching are the Google Scholar, Elsevier ScienceDirect, SpringerLink, IEEE Xplore, and ACM Digital Library. Moreover, it included the latest development of research papers from 2018 to 2025. Selection has been limited to peer-reviewed studies involving the Gen AI models like GANs, VAEs, and transformers. Each of the studies included in the data extraction has detailed specific model types, the characteristics of the datasets, and performance metrics. Based on the above data, the nature of Gen AI of IoT can be categorized as dual nature by identifying the opportunities and the challenges.

# Results or finding

Based on the result of this study, it can be seen as follows:

A summary of the Gen AI technologies that can be used for IoT security is provided in **Table 1**.

Gen AI technologies used for IoT security core mechanisms can be leveraged in various other security applications. Gen AI applications used for the key security applications can be leveraged from cryptography. The Gen AI can utilize GAN as a technology to provide competitiveness between the generator and discriminator and provide fake traffic to be used for security testing as well as IDS training. Another application of these technologies using latent space is compression of the data and reconstruction: Anomaly detection, outlier identification, edge-device failure monitoring. Gen AI: Sequence modeling, and natural language processing (NLP) are also technologies that leverage transformers and large language models (LLMs). Log Analysis, Automated Forensics, Malware Descriptions, and Security Triage. Gen AI diffusion models are regarded as a technology that "denoising" to generate data from "noise." Construction of very realistic synthetic data can improve that accuracy of the IDS.

To advance the security of IoT, there are various types of technologies that can be used by Gen AI.

There are different types of technologies that can be used by Gen AI for the security of IoT to make more advancement (**Table 2**). Can impersonate a user with his fake device and can access the network. The keys of the cryptography can be stolen; real and technical threats and analysis through use of side channels and power consumption can be measured, and loss of the wireless can be measured. Requests a computer load distributed denial of service (DDoS) threats to be distributed all over the world. Globally, the target computer is a server computer (Mirai botnet), giving it a load of thousands of stolen connections. Signals generated for communication—This will display the signals that are supposed to be used for communication along with ones that are threatening through radio frequencies. The devices in which the input data is available for machine learning (ML) can be modified. IoT environments are complex and distributed with a diversity of security needs. The heavy cryptographic methods have some drawbacks such as requiring a large memory, low CPU, battery dependent, etc., due to normal conventional cryptographic techniques.

IoT ecosystems are intricate, distributed networks with diverse security requirements. The usage of conventional heavy cryptographic techniques is constrained by resource limitations, such as low memory, low CPU power, and battery dependence (**Table 3**).

Potential threats and opportunities to the project: Opportunities, threats (the "risks"), record "zero-day attacks" (by identification), and the attacks that cannot be seen. The challenge here is this: After poisoning the model, it will tend to produce many false-negative results. Utilization with hardware such as CPU, battery, IoT devices can pose

**TABLE 1 |** Generative AI (Gen AI) technologies for internet of things (IoT) security.

| Technology | Core mechanism | Key security applications |
|---|---|---|
| Generative adversarial networks (GANs) | Competitive "Generator vs. Discriminator" model. | Synthetic traffic for intrusion detection systems (IDS) training, zero-day simulations, and robustness testing. |
| Variational autonomous coders (VAEs) | Data compression and reconstruction via latent space. | Anomaly detection, outlier identification, and edge-device failure monitoring. |
| Transformers and large language models (LLMs) | Sequence modeling and natural language processing. | Log analysis, automated forensics, malware descriptions, and security triage. |
| Diffusion models | Iterative "denoising" to create data from noise. | Generating highly realistic synthetic sensor data to improve IDS accuracy. |

**TABLE 2 |** IoT security landscape.

| Threat category | Specific attack type | Impact |
|---|---|---|
| Identity and access | Device spoofing | An attacker masquerades as a legitimate device to gain network access. |
| Physical/hardware | Side-channel analysis | Extracting cryptographic keys by measuring power consumption or electromagnetic leaks. |
| Network-wide | Distributed denial of service (DDoS) via Botnets | Can access several devices that have an object server that is loaded. |
| Wireless fidelity or radio waves | Looping and technique of jamming | By repeatedly sending the intercepted data packets via the communication, it can cause the system to malfunction. |
| Software/AI | Machine learning (ML) with counter productive | It has the ability to confound devices that have machine learning models and alter the supplied data. |

**TABLE 3 |** Opportunities and challenges.

| Category | Opportunities (the "upside") | Challenges (the "risks") |
|---|---|---|
| Detection | Identification of zero-day and unseen attacks. | High rates of false negatives if the model is poisoned. |
| Deployment | Self-healing and autonomous hardening. | Hardware limitations (CPU/Battery) on IoT devices. |
| Data | Synthetic data for robust training without privacy risk. | "Membership inference" where private data leaks into outputs. |

many challenges by installation; it is also a great way to practice caring about oneself as well as strengthening oneself. According to data, it will give an opportunity to train the data reliably without compromising privacy. The ability to disclose confidential information is called "membership inference." To know about Gen AI-enhanced IoT security, such as advanced threat and anomaly detection like zero-day attack identification, dynamic behavioral baselining and unseen attack discovery; about robust data management and privacy like synthetic data generation and high-dimensional data compression; about proactive and autonomous defense such as self-healing systems and automated system hardening (9, 14). Considering the prospect mentioned above, it can be concluded how Gen AI can be used to secure the IoT optimally with modern advancements.

In view of these difficulties, the Gen AI IoT course system has been enhanced with a multitude of security functionalities. It has also incorporated and assisted in ignoring numerous threats that are detrimental to the system's overall efficiency. By mitigating all these hurdles, offering comprehensive protection, adopting privacy-focused methods, and improving upon model efficiency, Gen AI can supply and further boost IoT security in a circular and effective way.

## Discussions

It is clear from this review that there are several challenges related to explainability, robustness, and privacy that must be addressed to fully exploit Gen AI and IoT security. In addition, in centralized model training, federated learning (FL) and safe multi-party computation (MPC) can be applied to protect data without revealing the raw data (9). Explainable AI approaches can be used to make sure that consumers acquire a more elevated degree of trust and transparency (11).

Moreover, the lightweight and energy-efficient design is essential for the operation of Gen AI on edge devices

with limited resources. Its integration with the real-time detection of intrusions, assessment of risks, and providing instantaneous protection makes Gen AI-powered agents significant in IoT cybersecurity. The significance of robust governance and ethical guidelines for harnessing such risks is therefore quite substantial, as Gen AI technology holds a vast potential to greatly improve IoT security, privacy, clarity, and moral control.

## Conclusion

Gen AI offers an independent security response adoption and is providing the widest revolutionary security opportunity in IoT. Inspecting traditional security of IoT security reveals that it is far away from the modern ones like accurate threat modeling, advanced anomaly detection, generation of synthetic data, and prediction of malicious behavior. The latest breakthrough in IoT is that it has enabled the information technology (IT) industries of smart cities, manufacturing, health care, transportation, and so much more. Hence, one of the crucial factors that determine the industry's efficiency would be associated with Gen AI. In addition, there are various obstacles when it comes to deploying Gen AI and IoT security, such as adversarial data position manipulation, privacy concerns for sensitive data, information and data leakage, malicious issues that could occur due to misuse of Gen AI, automated scripts that could cause vulnerabilities, etc. They need to use standard architectures and strict model design and deployment practices to properly counter all of these threats and weaknesses. Additionally, end-to-end low-complexity architectures (for a cloud-independent future) should be emphasized in the future. Moreover, differences between data location and manipulation should be distinguished by adopting the thieves' training techniques. Moreover, by guaranteeing the security and ethical applications of AI deployments, Gen AI promises the highest potential to ensure the wider adoption of IoT cybersecurity in more agile and adaptive escalation efforts.

## Funding

The author declares that no financial support was received for the research, authorship, and/or publication of this article.

## Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## References

1. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. *IEEE Int Things J.* (2022) 1(1):22–32.
2. Zhou H, Wen L. IoT cyber threat review. *Comput Secur.* (2022) 115:102620.
3. Goodfellow IJ, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y. Generative adversarial nets. In: Ghahramani Z, Welling M, Cortes C, Lawrence ND, Weinberger KQ editors. *Advances in Neural Information Processing Systems 27 (NIPS 2014)*. Red Hook (NY): Curran Associates Inc (2014). p. 2672–80.
4. Chen Y. VAE-based anomaly detection. *ACM Trans Database Syst.* (2021) 46(3):1–25.
5. Luo J. IoT vulnerabilities and botnets. *Comput Secur.* (2021) 103:102—116.
6. Wang X, Li Y. GAN-based intrusion detection for IoT. *IEEE Access.* (2023) 11:1–12.
7. Huang Z. Transformer-based threat intelligence. *IEEE Trans Neural Netw Learn Syst.* (2023) 34(9):7850–65.
8. Gupta R. Large language models for log analysis. In: *Proceedings of IEEE Big Data* (2024). p. 140–52.
9. Rahman F. Federated IoT security frameworks. In: *Advances in IoT Security*. Springer (2023). p. 15–32.
10. Patel K. AI-enhanced IoT defense systems. *Sensors.* (2022) 22(18):6501.
11. Kim M. Security risks of generative AI models. *ACM Comput Surv.* (2024) 57(4):1–32.
12. Roy S, Ahmed I, Khan M. Generative AI for cybersecurity. *IEEE Trans Inform Forensics Secur.* (2024) 19:501–15.
13. Bender A, Taylor M. The ethics of generative AI. *ACM Trans Priv Secur.* (2024) 27(2):1–18.
14. Das P, Roy R. Deep generative anomaly detection. *Neural Comput Appl.* (2023) 35:11289–305.