E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 04-10-2024
Accepted: 17-11-2024
Published: 06-01-2025

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 3; Issue 1; 2025; Page No. 454-460

Artificial Intelligence-Based Intelligent Intrusion Detection in Cloud Computing Settings

[1]Sreedhar Korubilli and [2]Dr. Shashank Naidu

[1]Research Scholar, YBN University, Ranchi, Jharkhand, India
[2]Associate Professor, YBN University, Ranchi, Jharkhand, India

DOI: https://doi.org/10.5281/zenodo.21918556

Corresponding Author: Sreedhar Korubilli

Abstract

The development task's stated goal was to investigate potential uses of machine learning methods for anomaly and malicious pattern detection in network data. The performance of these models on several publicly accessible benchmark datasets was also to be evaluated. For this study, we used four datasets that stand in for various types of networks and attacks: NSL-KDD, UNSW-NB15, CICIDS2017, and ToN_IoT. The data was preprocessed using a thorough pipeline that included reduced dimensions, trained several ML and DL models, and then compared and evaluated their performance in binary and multiclass classification. We tested many different models, including k-Nearest Neighbors, Decision Tree, Multi-layer Perceptron, Random Forest, Support Vector Machine, Logistic Regression, and Long Short-Term Memory networks.

Keywords: Cloud Security, Machine Learning (ML), Cyber Threat Detection, Real-Time Intrusion Detection, Network Security

Introduction

The introduction of digital platforms and smart automation has caused a dramatic shift in the financial services industry. More and more, complex machine learning models are driving financial applications such as risk assessment, algorithmic trading, credit scoring, and fraud detection. An up-to-date method of deployment is required for these models because of their requirements for high availability, scalability, processing in real-time, and strong security. To keep up with the performance standards set by consumers and financial institutions in this rapidly changing digital age, old-fashioned model hosting and batch-processing approaches are inadequate. The development, deployment, and scaling of financial applications have been radically altered by the advent of cloud-native technology. Organizations can now integrate, deploy, and monitor models at scale constantly with little downtime thanks to containerization, orchestration technologies like Kubernetes, and serverless infrastructures. In addition to facilitating dynamic scaling and isolating microservices, these advancements allow teams to produce models more quickly and with more leeway. There are a number of challenges associated with using old deployment methods for production model deployment, including a lack of insight into model performance over time, weak rollback procedures, and insufficient version control.

End-to-End Encryption

The secrecy of data is guaranteed by implementing comprehensive encryption measures at rest, in transit, and during processing, such as homomorphic encryption. User roles should inform key management, which should be decentralized.

Identity and Access Management (IAM)

Integrated access management (IAM) solutions limit user access to critical resources by enforcing the concept of least privilege. Additionally, insider risks may be mitigated via the use of Just-In-Time (JIT) access control and Privilege Access Management (PAM).

Intrusion Detection and SIEM

To monitor incident responses across several settings and identify suspicious activity, modern cloud security makes use of SIEM and Intrusion Detection Systems (IDPS).

Secure APIs and DevSecOps

Encryption, input validation, and robust authentication are essential for API security. The goal of DevSecOps is to decrease deployment vulnerabilities by incorporating security into the software development lifecycle.

Intrusion Detection Systems

Software and hardware intrusion detection systems (IDSs) automate the process of monitoring and analyzing events happening in computer systems or networks for signals of security concerns. Intrusion detection systems are now an integral part of most companies' security architecture due to the dramatic rise in both the frequency and severity of network assaults in recent years. For individuals who require an overview of intrusion detection, this document aims to cover the following topics: the security goals served by intrusion detection mechanisms, how to choose and set up an intrusion detection system for a particular system or network, how to handle the results generated by an intrusion detection system, and how to incorporate intrusion detection into the overall security architecture of an organization. If the reader needs more particular or expert assistance on intrusion detection, they may find references to alternative resources in the bibliography.

An intrusion is any effort to undermine the confidentiality, integrity, or availability of a computer system or network, or to circumvent its security measures. Intrusion detection is keeping an eye on system or network events and evaluating them for indications of intrusions. Intrusions may occur when unauthorized individuals get access to the systems over the Internet, when permitted users try to obtain new rights without proper authorization, or when approved users abuse their privileges. Automating this monitoring and analysis process is the job of Intrusion Detection Systems (IDSs), which may be either software or hardware solutions.

Classification of Intrusion Detection Systems

In a production network, there are several methods to categorize the different kinds of intrusion detection systems. For example, a signature-based method to detection might be used by a network-based intrusion detection system; these categories are not mutually exclusive. The following graphic illustrates the most prevalent approaches to IDS classifications; however, this is by no means an all-inclusive list.

Host-based IDS

Intrusion detection systems (IDS) that typically function within a computer, node, or device are known as host-based IDS (HIDS). Although several HIDS variations have been created for use in network monitoring, its primary use is internal monitoring. A computer, node, or device's internals are mostly what it watches and analyzes. According to de Boer and Pels (2005), HIDS alerts administrators when they detect a hacked system. For instance, it may identify malicious software that makes unusual requests to system resources or find software that has made dangerous changes to the registry.

Network-based IDS

Unlike HIDSs, which are often installed along a LAN cable, network-based IDSs (NIDSs) are positioned within the network itself. Through the examination of data packets en route to various sites, it seeks to identify malicious or unauthorized access to a local area network (LAN). Algorithms abound for identifying malicious traffic, but most of them scan incoming and outgoing packets for unusual behavior. A NIDS may inform administrators or take proactive measures, such banning the originating IP address, in response to any alarm it receives.

Direct port-to-port connection, network tap, and online connectivity are the three most frequent ways to install NIDS.

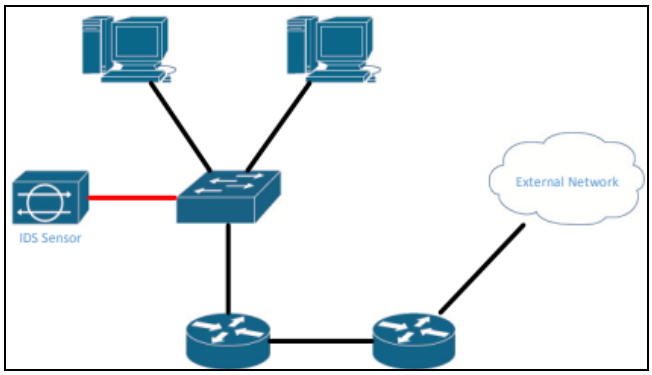

Fig 1: IDS using a switch spanning port

The IDS is shown in Figure 1 coupled with a switch that may be configured via its SPAN ports. According to Baker, Beale, Caswell, and Poor (2004), a SPAN port on some controlled switches has the ability to direct all network traffic to that port regardless of their final destination. Under this setup, the switch forwards all incoming traffic to the interface that is being utilized by the intrusion detection system. Since the switch has to work twice as hard to send data, the biggest drawback of this strategy is that it increases bandwidth and resource utilization.

Because of the security risks, hubs are no longer used by most current LANs. System communication that is not intended for a hub may be intercepted by hubs. The internal network systems are not vulnerable to an intrusion detection system (IDS) going down when a hub or switch with SPAN port capability is used. The SPAN port of a switch is a typical way that sensors are connected.

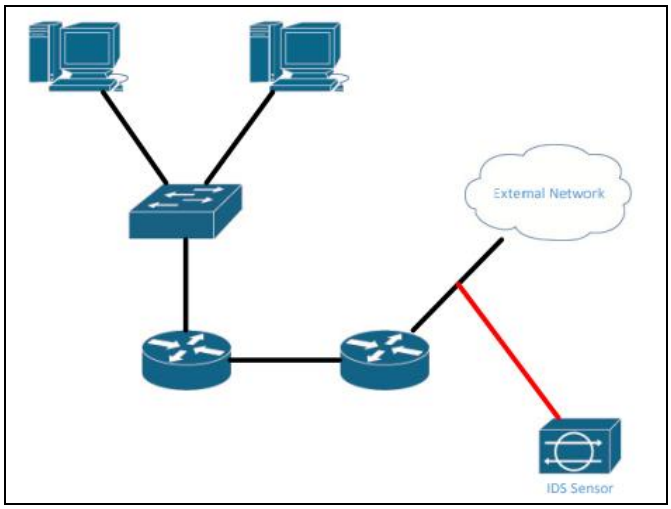

Fig 2: IDS using network tap

A network tap, as shown in Figure 2, allows an intrusion detection system to basically copy data that has been sent across a wire. You can buy network taps; however they aren't usually present in regular computer networks. When troubleshooting an issue or temporarily deploying an intrusion detection system (IDS), taps come in helpful for network administrators who need to put up a monitoring solution quickly. In general, a network tap is necessary in situations when the network lacks-controlled switches, is not using hubs, or where it would be prohibitive to install an intrusion detection system inline.

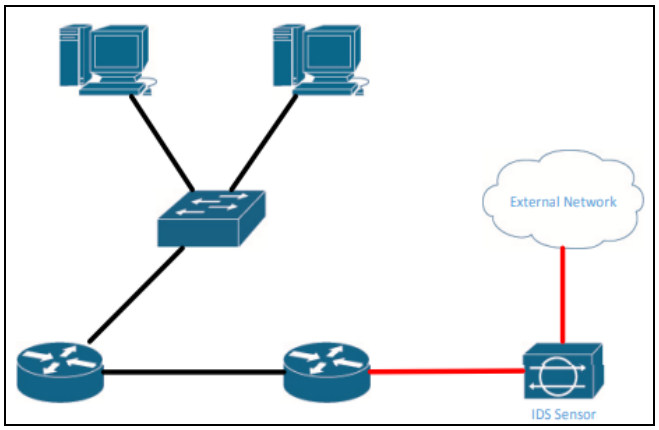

Fig 3: IDS connected inline

The red-labeled connections in this case go to the switch's uplink port and the external network, respectively. This is usually not the way to go since if the IDS goes down, all communication between the internal network and the outside world would be cut off.

On the other hand, with inline setup, you can be sure that the IDS will see every packet. When an intrusion detection system (IDS) is linked to a switch's SPAN port, packets may be overlooked, particularly if the switch is dealing with a high volume of traffic all at once. If a network sniffing protocol fails to record missed communication, it might be lost indefinitely. Congestion in network performance might result from a comparable burst, depending on the capabilities of an inline IDS.

Despite their usefulness, NIDSs come with a number of drawbacks when it comes to monitoring network traffic. It is possible to defeat NIDSs using common evasion tactics including session splicing, fragmentation assaults, and denial-of-service (DoS) attacks. Unencrypting a message in transit is not something a passive NIDS can perform if host-to-host connections are encrypted.

Importance Of Intrusion Detection Systems (IDS)

Security technologies that enable intrusion detection (ID), which captures for detecting unwanted access, intrusion, and abnormalities, include intrusion detection systems (IDS), both network-based and host-based. In order to safeguard sensitive information, keep the network intact, and detect any security breaches in real-time, it is crucial to analyze these interactions using an intrusion detection system. When an intrusion detection system (IDS) identifies potentially harmful activity, such as unusual download patterns, malware infections, or attempts at unauthorized access, it can begin to respond in real-time by sending out alerts and detailed logs that allow for swift action to be taken against the threat. Organizations may ensure compliance with data protection rules during audits by logging network activity that are detected by intrusion detection systems.

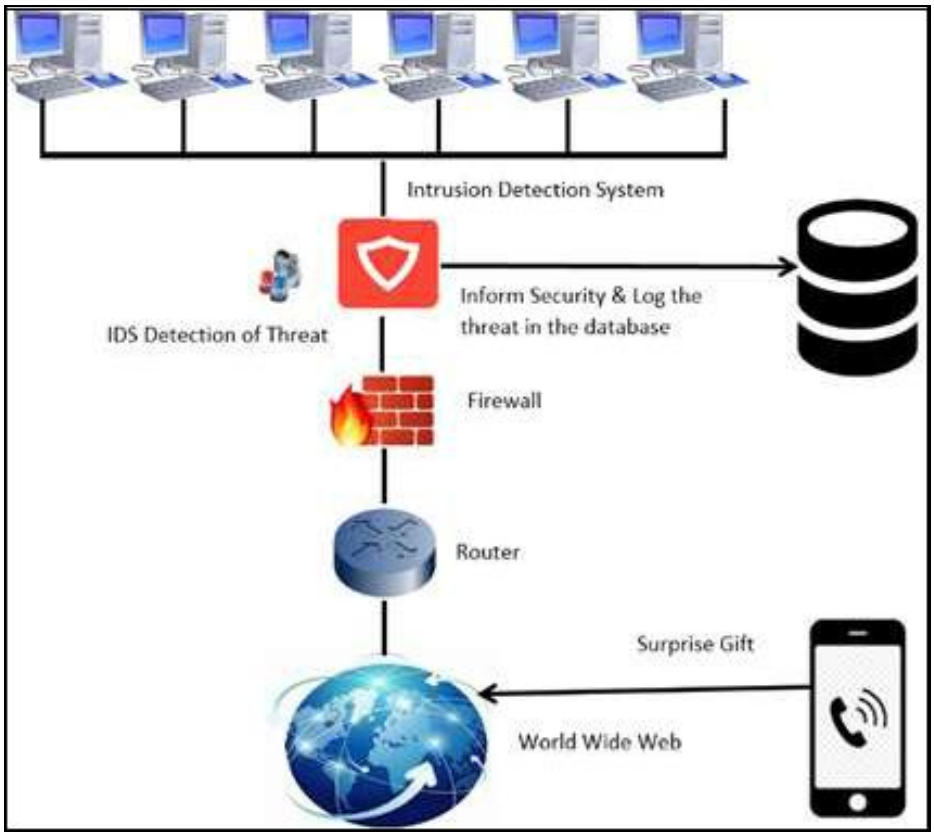

Fig 4: Intrusion Detection System in General

In addition, they let you see what's happening on your network, which means you can see things like user activity and traffic patterns, which may help you strengthen your company's security measures.

Identifying suspicious activity and abuse of a network is the primary goal of intrusion detection systems. Although intrusion detection has been available for about 20 years, its integration into information security infrastructure and general appeal have just lately seen a meteoric surge. Written for a government agency in the 1980s, James Anderson's groundbreaking work established the idea that audit trails held important information that may be used for detecting abuse and analyzing user behavior. The idea of "detecting" abuse and certain user actions came to light with the publication of Anderson's study. Both host-based intrusion detection and intrusion detection systems were born out of his research. Intrusion detection methods started to be developed commercially in the 1990s. The first commercial provider of intrusion detection system (IDS) tools was Haystack Labs, with its Stalker host-based product line. Computer Misuse Detection System (CMDS) was another kind of host-based intrusion detection that SAIC was working on. Concurrently, the Automated Security Measurement System (ASIM) was built by the Air Force's Crypto Logic Support Center to monitor traffic on the US Air Force network.

Role of Gen AI in Intrusion Detection

Gen AI is a new and exciting paradigm in artificial intelligence that goes beyond basic machine learning to let computers do things like generate data, mimic assaults, and adjust their detection models based on new information. Gen AI methods like Generative Adversarial Networks (GANs) and Large Language Models (LLMs) enable IDS to adapt to new and complex cyber threats in real time, as opposed to traditional supervised systems that depend mostly on labeled datasets.

Gen AI's capacity to provide synthetic data for training is a major asset to IDS. There is a shortage of complete datasets that record zero-day vulnerabilities, insider threats, or multi-vector assaults in many dynamic cloud infrastructures. To improve detection models' resilience, GANs may generate realistic attack traffic, which addresses data imbalance and augments underrepresented classes. Adaptive defensive systems may be enhanced by combining reinforcement learning with generative modeling to mimic hostile behavior. LLMs provide context-aware analysis by processing heterogeneous data sources such as logs, configurations and network telemetry.

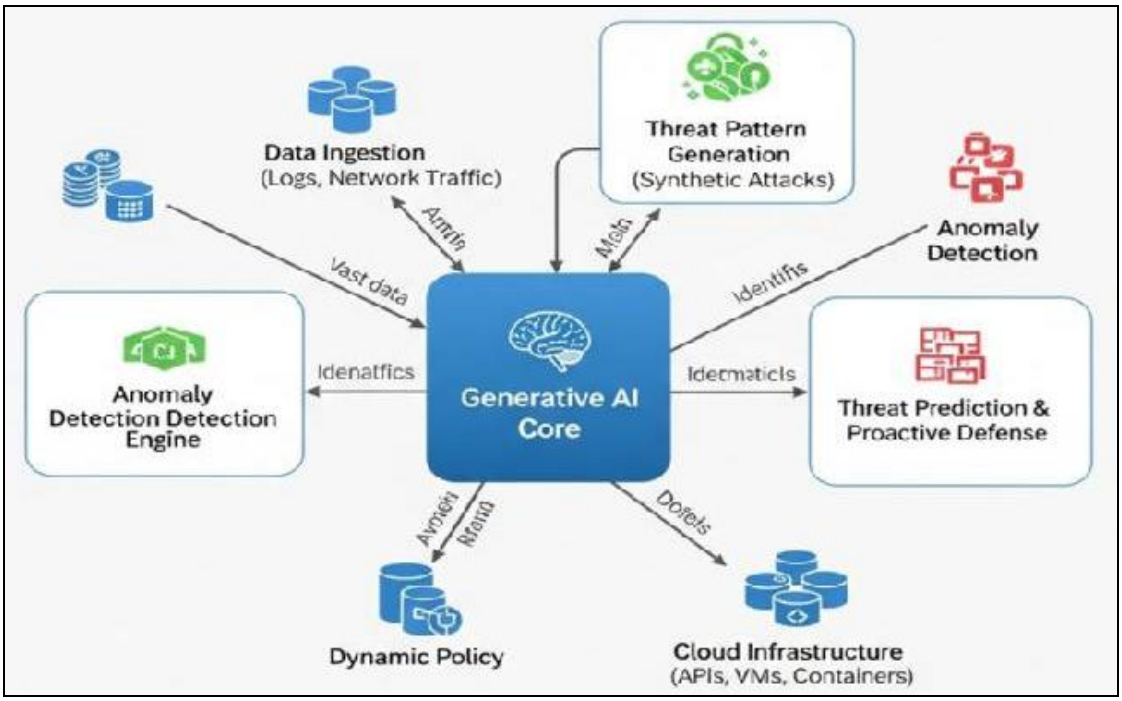

Fig 5: Gen AI in Intrusion Detection.

New research shows that LLMs can identify small irregularities, decipher event sequences, and provide solutions with little to no human input. Intruder detection systems may then progress from passive monitoring to proactive security frameworks powered by intelligence. Gen AI-based adversarial training fortifies IDS defenses against evasion attempts. In order for systems to better predict changing threat environments, models are continually exposed to samples that are created by adversaries. With its generative-adaptive cycle, Gen AI is set to become the backbone of next-gen IDS in contexts with a lot of change, hybridization, and several clouds.

Architecture of a Gen AI–Driven IDS for Cloud

A Gen AI-driven Intrusion Detection System (IDS) built for the cloud has to be cloud-native, modular, and very scalable so it can handle workloads that are always changing across different cloud and hybrid infrastructures. Gen AI enabled architectures provide adaptive learning and self-evolution, in contrast to conventional intrusion detection systems (IDS) that depend on fixed detection pipelines.

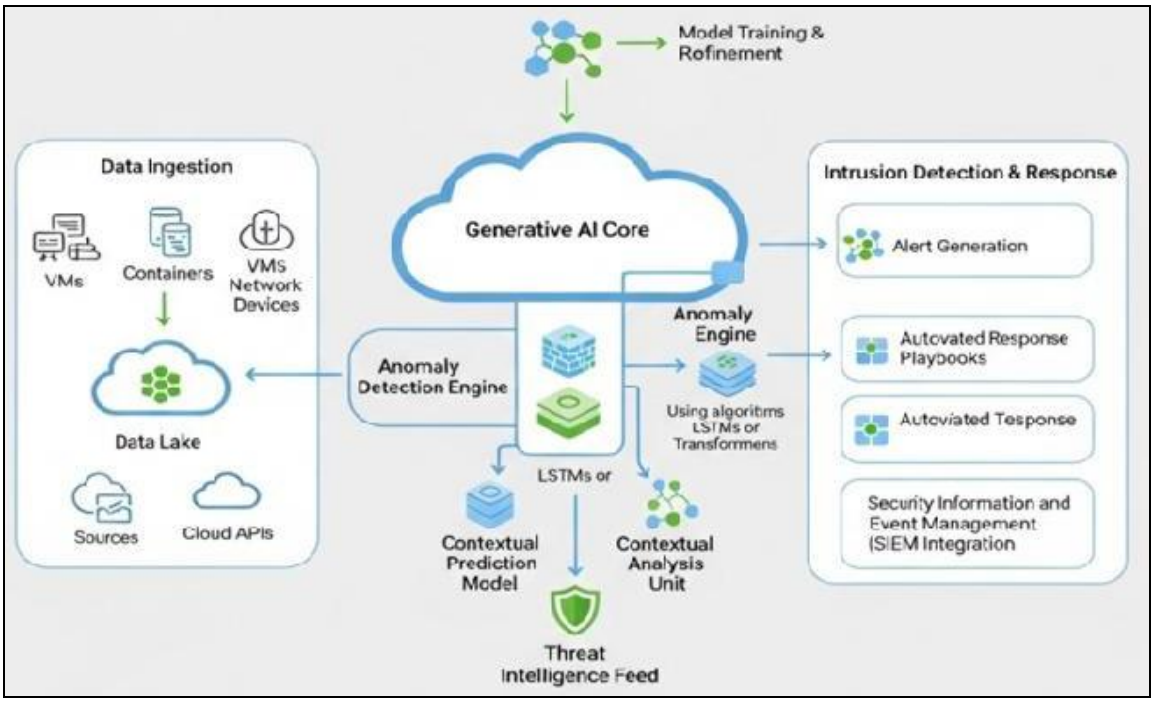

Fig 6: Architecture of a Gen AI–Driven IDS for Cloud.

Use Cases and Applications

Numerous real-world uses in ever-changing cloud settings are made possible by incorporating Generative AI into Intrusion Detection Systems (IDS). These examples show how Gen AI improves cybersecurity by making systems more resilient, adaptive, and able to foresee and counteract cyberattacks.

Real-time detection of zero-day exploits

Finding vulnerabilities that have not been publicly disclosed is a major obstacle to cloud security. In order to train intrusion detection systems, Gen AI models may mimic previously unknown attack pathways and create synthetic exploit behaviors. According to research, GAN-based models outperform traditional anomaly detection approaches when it comes to spotting new types of threats.

Insider threat detection

Because of their nuanced and context-dependent character, insider assaults continue to be challenging to detect. Intrusion Detection Systems (IDS) may examine logs, user actions, and communication patterns with the use of Large Language Models (LLMs) to spot irregularities that might mean data exfiltration or privilege abuse. Context-aware analysis detects more nuanced behavioral abnormalities with fewer false positives.

Multi-vector attack detection across clouds

Cloud workloads are vulnerable to dispersed and coordinated assaults because they often span hybrid and multi-cloud infrastructures. Improved detection accuracy in dispersed contexts is made possible by Gen AI, which allows IDS to correlate heterogeneous telemetry data and simulate complicated multi-vector assaults.

Automated red teaming and threat simulation

Attack scenarios that imitate adversarial tactics, methods, and procedures (TTPs) may be automatically generated using generative models. This functionality enhances intrusion detection system training and enables proactive red teaming for ongoing security validation.

Integration with DevSecOps pipelines

Organizations that operate entirely in the cloud require CI/CD procedures that include continuous monitoring. To make sure that new applications can withstand new attacks, AI-driven IDS may provide synthetic test cases, adaptive policy updates, and automated feedback loops for DevSecOps pipelines.

Benefits Of Current Ai in Ids for Iot Networks

Using AI in an IDS has several benefits, especially for low-resource IoT networks. A major benefit of AI models is the improved detection they provide. They have the ability to learn and adapt to constantly evolving dangers, which improves their ability to identify assaults that were previously undiscovered. Threat detection with AI models is more accurate and reliable than with conventional IDS because of the lower false positive rates.

Use of AI in IDS also has the added benefits of being efficient and scalable. Even artificial intelligence algorithms may be fine-tuned to operate on Internet of Things devices with limited resources, such as memory and computing power. Responding (in real-time) to traffic analysis and swiftly mitigating potential risks also requires machine learning and deep learning skills for real-time processing.

Challenges Of Securing Iot Networks

An enormous obstacle is the security of IoT networks. Limited resources are a big problem. Traditional security techniques, such encryption, might be challenging to apply on many IoT devices due to their limited computing capacity and energy. They are thus open to assault because of it. Due to the diverse security requirements of the many

devices that make up the Internet of Things (IoT), scalability poses an additional challenge to security as the number of IoT devices continues to increase. The multiplicity of devices-which include all other types of hardware, software, and communication protocols-is preventing the establishment of universal security standards.

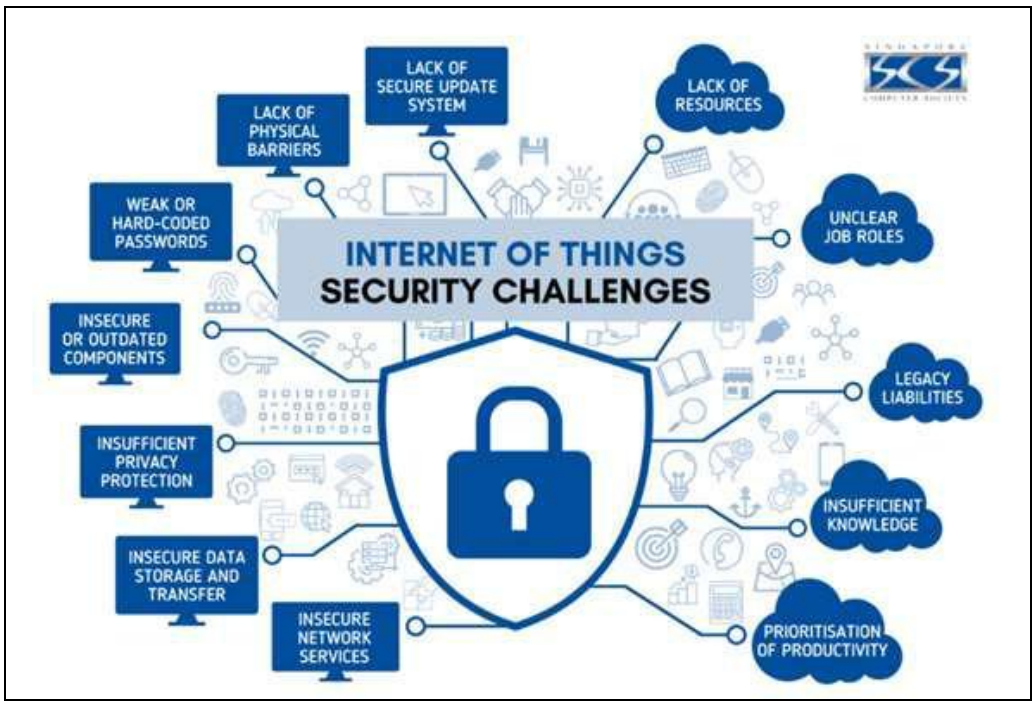

Fig 7: IoT security challenges

Furthermore, because to their dispersed nature, IoT devices are vulnerable to assaults like distributed denial of service (DDoS) as well as physical manipulation. The integrity of personal information and the possibility of unintended or malicious unauthorized access are two privacy issues exacerbated by massive data sets. Lifecycle management is complex, since many devices are not likely to get regular upgrades, leaving them vulnerable to new threats. In security, non-standardization leads to inconsistent protection. The integration of these security functions into the relevant IoT network cannot be accomplished without a thorough set of standards, together with lightweight security protocols and strong authentication mechanisms. This is to ensure that the capabilities and innovation intended by the IoT are not compromised.

Conclusion

Recurring worries included a lack of teaching examples, which might lead to the omission of uncommon but damaging attack types due to class imbalance. Inadequate data for specific dangers persists regardless of how sophisticated an algorithm becomes; this highlights the need for data-centered solutions, such as synthetic data production or cross-organizational data sharing, in tandem with algorithmic advancements. Deploying AI-IDS into the real world will need continuous learning and tweaking since we also ran into the problem of model generalization, which is when a model learned in one environment doesn't automatically work in another. Furthermore, our models may have done enough on benchmarking data, but the complexity and prevalence of zero-day attacks in real-world network traffic makes this data set irrelevant. For this reason, it is recommended to include an AI-powered intrusion detection system (IDS) into an existing security architecture that also includes anomaly detection and is overseen by human analysts in order to discover really unique patterns.

References

1. Manimaran M, Ranganathan S. AI powered cybersecurity frameworks for intrusion detection and threat intelligence in smart infrastructure. 2025. doi:10.71443/9789349552357-11.
2. Mohamed Shaffi S, Vengathattil S, Nikarthil Sidhick J, Vijayan R. AI-driven security in cloud computing: enhancing threat detection, automated response, and cyber resilience. 2025. doi:10.2139/ssrn.5212904.
3. Uddoh J, Ajiga D, Okare B, Aduloju T. AI-based threat detection systems for cloud infrastructure: architecture, challenges, and opportunities. Journal of Frontiers in Multidisciplinary Research. 2021;2:61-67. doi:10.54660/IJFMR.2021.2.2.61-67.
4. Narang S. Zero-trust security in intrusion detection networks: an AI-powered threat detection in cloud environment. International Journal of Scientific Research and Management. 2025;4(5). doi:10.38124/ijsrmt.v4i5.542.
5. Igulu K, Johnson B, Stephen A, Bhatia T. Security challenges in IoT. 2024. doi:10.1007/978-981-97-0052-3_4.
6. Wang F, Xie S. Cybersecurity in cloud computing: AI-driven intrusion detection and mitigation strategies. IEEE Access. 2025. doi:10.1109/ACCESS.2025.3580569.
7. Smith J, Kevin E. AI-powered intrusion detection systems for next-generation cloud. 2025.

8. Abbas G, Shah W. AI-enabled intrusion detection systems for secure multi-cloud environments. 2026. doi:10.13140/RG.2.2.34146.59842.
9. Johnson A, Townsend R, McCoy D. AI-based cybersecurity frameworks for enterprise cloud systems. 2025.
10. Cate M. AI-powered intrusion detection systems: challenges and opportunities. 2025.
11. Sangeetha KP, Shasikala P, Madhavi C. AI powered cybersecurity frameworks for intrusion detection and threat intelligence in smart infrastructure. 2025. doi:10.71443/9789349552081-11.
12. Lindsey O, College W, Mohammed O. AI-driven cybersecurity for cloud-based data systems: anomaly detection, threat mitigation, and performance optimization. 2025. doi:10.13140/RG.2.2.18277.10721.
13. Chamariya Y. The evolution of cyber security: AI and cloud technologies take the lead. International Journal of Intelligent Systems and Applications in Engineering. 2022;10:337-344.
14. Isabirye E. Cybersecurity framework for securing cloud and AI-driven services in small and medium-sized businesses. 2025;58. doi:10.5281/zenodo.15719943.
15. Hossain Z, Hossain M, Ahmed N, Kabir F, Hossain I. AI-powered framework for real-time threat detection and response in cloud infrastructure. Formosa Journal of Multidisciplinary Research. 2025;4:1859-1874. doi:10.55927/fjmr.v4i4.168.
16. Chunawala H, Chunawala P. Enhancing cybersecurity in cloud environments using AI-driven threat detection and response. International Journal of Futuristic Innovation in Engineering, Science and Technology. 2024;3:13-30. doi:10.59367/2420ra43.
17. Khan M. Developing AI-powered intrusion detection system for cloud infrastructure. Journal of Artificial Intelligence, Machine Learning and Data Science. 2024;2:1074-1080. doi:10.51219/JAIMLD/mohammed-mustafa-khan/255.