International Journal of Cyber Threat Intelligence and Secure Networking (IJCTISN)
eISSN: 3087-4297
Volume03 Issue07 | Page No: - 20-29

Received: 25 May 2026, Revised: 15 June 2026, Accepted: 26 June 2026, Published: 21 July 2026

DOI: https://doi.org/10.55640/ijctisn-v03i07-03

Survey of Artificial Intelligence-Driven Zero-Day Vulnerability Detection Techniques in Cloud Computing Systems

Dr.Jvalant Kumar Kanaiyalal Patel [1]

[1] Assistant Professor, Shri Manilal Kadakia College of Commerce, Management,Science and Computer Studies, Ankleshwar, India

ABSTRACT: The distributed design, virtualization, and multi-tenancy of cloud computing pose substantial cybersecurity concerns; however, it has become an essential technology for providing scalable and on-demand computing services. In particular, zero-day vulnerabilities pose a serious threat as they take advantage of undiscovered software defects prior to the release of security fixes, rendering traditional signature-based defense techniques useless. By facilitating intelligent threat detection, anomaly identification, and automated reaction, artificial intelligence (AI) has arisen as a potential solution to tackle these difficulties. A thorough examination of AI-driven methods for detecting zero-day vulnerabilities in cloud computing settings is provided in this article. It takes a look at cloud security basics, zero-day vulnerability lifecycle and effect, and new machine learning (ML), deep learning (DL), and hybrid AI detection methods. In addition, the report analyses current research, compares current approaches, and finds important gaps in understanding how to scale, protect privacy, implement in real-time, and generalize to other types of attacks. The findings indicate that although AI-based approaches have significantly improved detection performance, further research is required to develop interpretable, robust, and scalable cybersecurity solutions capable of mitigating evolving zero-day threats in dynamic cloud environments.

KEYWORDS: Cloud Computing, Zero-Day Vulnerabilities, Cybersecurity, Artificial Intelligence (AI), Threat Detection, Anomaly Detection, Cloud Security.

1. Introduction

One of the basic technologies for providing scalable and affordable computing facilities through the Internet is cloud computing. Nowadays, cloud computing services are extensively used by companies to host their applications, keep secure information about their customers, and operate their businesses. Despite the benefits that cloud computing provides, it suffers from severe security problems because of its architectural features. These features include distributed nature, multi-tenancy, virtualization, and dynamic resource allocation. They broaden the attack surface and make cloud systems more vulnerable to such as malware, ransomware, insider attacks, DDoS attacks, and software vulnerabilities [1]. Zero-Day Vulnerability entails previously unknown software weaknesses that are attacked by hackers even before the developers come up with countermeasures to patch the security holes[2]. Zero-Day vulnerabilities lack known patterns of signatures and thus most security tools based on the same tend to be ineffective when combating them. In case of successful Zero-Day attack, this causes access to systems without permission, loss of information/data, financial implications, and system outages. Security in cloud computing relies on finding Zero-Day vulnerabilities early and fixing them [3].

The sophistication of Zero-Day vulnerabilities, together with the emergence of targeted cyber-attacks, has significantly raised the significance of identifying them. Because software businesses and security experts are unaware of zero-day vulnerabilities while they are being used, hackers have a leg up and may carry out destructive actions for long periods of time without anybody noticing. In the realm of cloud computing, a single Zero-Day vulnerability exploited affect virtual machines, containers, applications, or shared infrastructures and cause data leaks, monetary losses, disruption of operations, and harm reputation [4].

AI technology has turned out to be a revolutionary technology that allows for enhancing the cybersecurity of organizations through intelligent, adaptable, and automation-based detection of potential threats. With the application of such AI technologies as ML, DL, RL, and LLMs, huge amounts of security data can be processed in order to reveal any patterns of attacks, anomalies, and

forecast future cyber threats. Unlike the conventional security measures, AI-based technologies continue learning from the newly gathered information and adapting to changes in the strategy of attackers without any necessity to perform manual updates [5].

A. Structure of paper

The rest of this paper is organised in this way. Learning the basics of zero-day attacks and cloud computing is covered in Section II. Cloud environments and zero-day vulnerabilities are covered in Section III. Finding zero-day vulnerabilities is covered in Section IV, which focuses on AI-driven methods. The current research gaps in AI-based zero-day attack detection are highlighted in Section V, which also offers a thorough literature overview. The paper is finally concluded in Section VI.

2. Overview of Cloud Computing and Zero-Day Attack

With cloud computing, companies have gained a new way of deploying, managing, and accessing computing resources by using scalable, flexible, and affordable services via the Internet. The virtualisation, multi-tenancy, infrastructure dispersal, and dynamic resource allocation that come with cloud computing also pose new cybersecurity challenges. Typical security software, such antivirus programs that rely on signatures or intrusion detection systems that use rules, is ineffective against these kinds of assaults. Increases in the detection and response capabilities of current cybersecurity systems have been made possible by advancements in AI, which have greatly improved their efficiency [6].

A. Cloud Computing Security

This is a system that allows users to access shared computer resources including storage, networks, databases, software, and applications over the Internet whenever they need them [7]. Cloud computing differs from more conventional forms of computer hosting in five important ways.

- Users are able to experience the seamless availability of their computing resources through on-demand self-service, eliminating the need for direct vendor involvement.

- Cloud services may be accessed from a variety of devices, such as desktop computers, laptops, smartphones, and tablets, using the Internet protocols made possible by broad network connectivity [8].

- Resource pooling ensures that the computing resources can be pooled and shared across many users through a multi-tenant approach.

- Fast elasticity makes it possible to increase or decrease the amount of resources depending on the load.

- Measured services that automate the process of monitoring and accounting for resource usage to ensure that customers pay only for used resources[9].

The cloud computing system is scalable, adaptable, and cost-effective because of these properties; nevertheless, there are security concerns associated with these features, thus it is important to defend the system from various cyber-attacks, including Zero-Day attacks. [10].

B. Zero-day Attacks

A network administrator or software creator may not know about all flaws. If these vulnerabilities are used, they have no way to find out about them or protect themselves. Consumption of these services leaves consumers open to potential privacy-invasive threats or attacks. Unknown assaults like this are called zero-day attacks. A zero-day attack is practically impossible to prevent [11] due to the fact that the vulnerability is unknown, the impacted software cannot be fixed, and antivirus solutions cannot identify the attack using signature-based scanning. Figure 1 shows the potential vectors for a zero-day assault against software, networks, or systems.

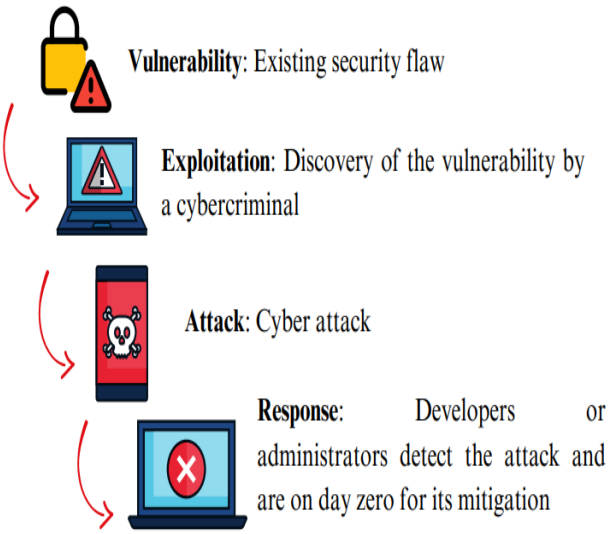

Fig. 1. Workflow of a zero-day attack [12]

The following is a detailed breakdown of the steps used to launch a zero-day attack:

- Vulnerability: The time between a system's vulnerability being found and a patch or fix being developed to address it is called the vulnerability stage in a zero-day attack. At this pivotal point, the system is open to hackers' assaults and exploitation [13].

- Exploitation: A zero-day attack's exploit phase involves taking advantage of a recently found software or system vulnerability before a remedy is developed. This part of the process entails breaking into the target

system without permission by making use of certain methods and tools to exploit the vulnerability.

- Attack: Once the flaw is exploited, the hacker gets unauthorized access to all data stored on the compromised system, including sensitive user information [14].

- Response: The software manufacturer often releases a security update that fixes the vulnerability that was exploited in the attack. To further reduce the likelihood of future assaults of this kind, it is possible to evaluate security policies, provide staff training, and enhance network monitoring.

3. Zero-Day Vulnerabilities in Cloud Environment

Cloud computing infrastructure in the modern era is vulnerable to cyber attacks such as zero-day vulnerabilities. The term Zero-Day vulnerability represents any previously undiscovered security hole in software, hardware, or operating systems that is exploited by a hacker before it gets detected by the software vendor and patched. The absence of any specific signs, security patches, and defense mechanisms makes the Zero-Day attack one of the hardest attacks to detect and protect against using traditional security tools. Such vulnerabilities cause great risks for cloud infrastructure by exploiting virtual machines, applications, databases, and shared resources causing data theft, financial losses, and downtime. The majority of the other cyber threats use known vulnerabilities, the Zero-Day attack targets previously unknown security holes. Traditional IDS, antivirus, and security solutions are mostly based on known patterns of attacks that make them ineffective against new attacks [15]. A series of steps that begin from the discovery of a vulnerability and end with recovery of a system when security measures are applied to the affected IT infrastructure. Businesses can better prepare for, identify, and counteract zero-day attacks in the cloud if they are aware of this lifecycle [16].

A. Vulnerability Discovery

The life cycle starts with the discovery by attackers of previously unknown security holes in software, operating systems, web applications, cloud infrastructure, and network systems. Such vulnerabilities can occur due to programming errors, bad designs, incorrect configuration, and any other factor.

B. Exploitation

Having found the vulnerability, attackers perform an analysis of its behavior and create code that exploits the vulnerability discovered. It allows bypassing all available security systems and can be distributed through phishing emails, malicious websites, software updates, APIs, etc [17].

C. Execution of Attack

In the attack execution stage, the vulnerability exploit is carried out on the target cloud infrastructure, applications, or networks. This allows attackers to carry out their nefarious actions such as gaining access to the system, privilege escalation, installing malware, carrying out ransomware attack, data stealing, denial of service or lateral movements through interconnected cloud resources.

D. Patch Release

The software provider immediately begins a thorough investigation into the vulnerability's origin and impact the moment it is discovered, either independently or through cybersecurity researchers or other impacted entities [18][19]. Then a security patch or software upgrade is developed and distributed to mitigate the threat from the said vulnerability. The time span from discovery of the vulnerability till the release of the patch exposes organizations to risks [20].

E. Impact of Zero-Day Vulnerabilities on Cloud Computing

Cloud computing poses a serious concern since it takes advantage of undiscovered security gaps. As a result, the makers of the impacted software have not made fixes accessible. The fact that cloud computing is highly dynamic and distributed means that any vulnerability can be easily exploited by cyber attackers to cause severe harm. Apart from the technical problems created by a Zero-Day vulnerability, there are several other negative implications such as financial, operational, legal, and reputational issues [21]. Major Impacts of Zero-Day Vulnerabilities:

1) Unauthorized Access of Cloud Resources:

The attacker uses the flaw to bypass identity and authorization systems. This lets them get into cloud resources like computers, virtual machines, databases, storage, and other administrative tasks without permission [22].

2) Breaches of Confidential Data and Information Leaks

Zero-day exploits usually target confidential business data, financial records, healthcare information, intellectual properties, and personally identifiable information (PII) stored in the cloud environment causing serious breaches of privacy and legal issues.

3) Deployment of Malware and Ransomware

Zero-day exploits often facilitate the installation of

malware, ransomware, spyware, or backdoors in cloud computing environments that cause harm such as encryption of vital data, disruption of business operations, theft of confidential data, and providing a means for future exploitation [23].

4) Service Interruption and Denial of Service Attacks

Using zero-day exploits to interrupt the availability of cloud services through crashing of the application, disabling of vital infrastructure, and launching of DDoS attacks.

5) Financial Loss and Operational Disruptions

Business entities that face Zero-Day attacks tend to suffer considerable financial loss as a result of costs incurred in recovering from system failures, costs associated with incident response, regulatory fines, legal liabilities, and disruptions to business activities [24].

6) Customer Trust and Reputation Loss

When there is a security breach from Zero-Day vulnerability, reputation can be badly hit. Customers might not trust organizations any longer due to their inability to secure their sensitive information. This could lead to revenue reduction and loss of customers.

7) Regulatory Compliance Failure

Most industries need to abide by cybersecurity standards like GDPR, HIPAA, PCI DSS, and ISO/IEC 27001. When a zero-day attack exposes sensitive information, there would be non-compliance with regulatory requirements, legal action, financial penalties, and even security audits [25].

8) Lateral Spread on Cloud Workloads

The cloud environment is usually highly connected because of virtual machines, containers, microservices, and shared infrastructure. After the attack through Zero-Day exploit, attackers spread laterally within cloud workloads to compromise more systems [26].

9) Expanded Attack Surface for Multi-Cloud Architectures

To enhance scalability and availability, enterprises adopt a multi-cloud environment where applications run on different cloud platforms. Unfortunately, the use of a multi-cloud architecture complicates the design and increases the attack surface by offering numerous opportunities for hackers to take advantage of weaknesses within interconnected systems.

10)Security Threats Over Time

Should the zero-day weaknesses be left unnoticed over time, the hacker continues to have sustained access and steals sensitive data, manipulates cloud computing infrastructure, or perpetuates other attacks without getting detected. It makes incident response a challenge and poses security threats in cloud computing environments [27]. Table I shows the comparison between security and zero-day threats.

TABLE I. COMPARATIVE SUMMARY OF CLOUD COMPUTING SECURITY AND ZERO-DAY THREATS

Topic	Description	Security Challenges	AI Relevance
Cloud Computing Security	Internet-based computing using scalable resources	Multi-tenancy, virtualization, insecure APIs	Intelligent security monitoring
Cloud Service Models	IaaS, PaaS, SaaS	Different security responsibilities	AI-based risk assessment
Cloud Deployment Models	Public, Private, Hybrid, Community	Shared infrastructure risks	Automated security management
Zero-Day Vulnerabilities	Unknown software flaws exploited before patches	Difficult to detect using signatures	AI-based anomaly detection
Zero-Day Attack Lifecycle	Discovery, Exploitation, Execution, Patch	Delayed detection and response	Early prediction and mitigation

4. Zero-Day Vulnerability Disclosure and Patching

Protecting against such threats requires the disclosure of zero-day vulnerabilities and the following patch rollout. Notifying software vendors of a vulnerability and giving them enough time to remedy it is essential [28][29]. Disclosing zero-day vulnerabilities and the challenges of timely patch releases are topics covered. The term "responsible disclosure" describes the proper and coordinated way to notify software developers and other stakeholders of security vulnerabilities. For vendors to have enough time to address the vulnerability before the information is made public, researchers who discover zero-day vulnerabilities usually adhere to responsible disclosure protocols. As a rule, the following procedures are involved in responsible disclosure:

- **Notification**: A zero-day vulnerability is reported to the impacted vendor or relevant entity by the researcher. Included in this alert is comprehensive data on the vulnerability, its effects, and any applicable proof-

of-concept code or examples [30].

- **Coordination**: The vendor and researcher collaborate to verify and comprehend the vulnerability. In order to resolve any issues or queries, this may need more dialogue, the exchange of new details, or teamwork [31].

- **Public Disclosure**: The researcher may decide to make the vulnerability public after a fair amount of time has elapsed to enable consumers to apply the fixes. Making people aware of the situation and the need to implement the fixes is top priority.

- **Patch Release**: The vendor makes the fixes available to the public once they are ready. Release notes or security warnings usually accompany this, outlining the vulnerability, its effect, and how users may install the fixes.

- **Patch Development**: The vendor takes care of fixing the issue by creating patches or security upgrades. Thorough testing and quality assurance may be incorporated into this procedure to guarantee that the patches successfully address the vulnerability without creating any additional problems.

5. Ai-Driven Zero-Day Vulnerability Detection Techniques

With the development of cyberattack technologies, Zero-Day vulnerabilities have become one of the major cybersecurity problems to address. As Zero-Day vulnerabilities are used in cyberattacks before any patches to software, companies need advanced and intelligent security systems that can recognize unknown threats in real time. At the same time, AI becomes an interesting approach to tackle this challenge, providing an intelligent analysis of data, decision-making, and self-learning of the technology. AI security systems analyze big amounts of data generated in cloud, including network traffic, system logs, user activity, and application behavior to find hidden attacks and emerging cyber threats[32]. AI has emerged as an important element of cloud security by offering intelligent and automated defense mechanisms that are able to counter the increasing complexities in cloud computing environment. AI technology helps overcome these weaknesses by making use of ML, DL and behavioral analytics in analyzing large volumes of security data [33].

A. Machine Learning-Based Vulnerability Detection

One of the most popular Artificial Intelligence technologies is used to detect Zero-Day vulnerabilities in cloud computing environment. ML learns the patterns from the security data and makes distinction between normal and malicious activities in the system without programming it. ML uses the data related to network traffic, logs, user activities and applications to find the anomalies that suggest Zero-Day attacks[34].

B. Deep Learning-Based Threat Detection

This is a type of ML approach that uses multi-layered NNs to automatically extract features from security data sets. This method of threat detection is an improvement on ML-based threat detection because the DL algorithm uses several layers of neural networks in extracting the features from the high-dimensional security data without manual engineering as happens in conventional ML algorithms. DL is best suited for Zero-Day vulnerability detection due to the nature of high-dimensional cloud security data [35].

C. Hybrid AI Models for Zero-Day Detection

Models employ several techniques of Artificial Intelligence or use Artificial Intelligence in conjunction with conventional security solutions to detect zero-day exploits more effectively. Hybrid models make the best of ML, DL rule-based approaches, signature-based detection, and ensemble learning to ensure better accuracy and reliability. Hybrid models are especially useful for cloud computing where it is necessary to examine several streams of information at once and mitigate the limitations of individual models.

6. Literature Review

This section provides a survey of previous work that has been done on a comparable subject and keywords that are relevant to it.

Cherng En et al., (2026), utilize a next-generation framework of cyber defense based on DL intrusion detection and a cloud-native security orchestration and automatic response mechanisms. The system takes advantage of hybrid CNN-LSTM models that are deployed as Kubernetes-based microservices to provide scalable, adaptive, and intelligent threat detection. The results of the experiment outperform the results obtained using conventional ML and signature-based methodologies in terms of accuracy, precision, recall, and F1-score. The architecture is consistent with the current DevSecOps and AI-enabled cloud engineering paradigms, which guarantee scalable and resilient cyber protection [36].

Malkawi and Alhajj, (2026), suggest that, when contrasted with rule-based and human-driven solutions, AI technologies significantly enhance detection precision, scalability, and reaction time. The shift from traditional ML classification to doing source code analysis and dynamic network identification with DL. Also, find out about cutting-edge mitigation tactics including AI-driven prioritization, neuro-symbolic AI, deep RL, and LLMs' generative capabilities for automated patch recommendations. Transparent screening judgments and

repeatable database searches (including specific queries and search dates) are reported to increase methodological rigor in this review. The research was selected using a PRISMA-based strategy and followed a recognized methodology. Improvements in AI-driven vulnerability management throughout the years suggest that the technology's successors need to be more open, resilient, and generally applicable in addition to being more precise [37].

Manjula and Saravanakumar, (2025), cloud security threat detection systems utilizing Zero-Day should primarily focus on ML and DL techniques. Feature engineering, anomaly detection, and hybrid models that integrate conventional security protocols with cutting-edge AI methods to enhance detection precision are therefore highlighted in the survey. Large datasets are required, false positives are a problem, and interpretability is a hurdle; these and other implementation issues are discussed in the review. It also shows how crucial it is for detection systems to learn and adapt over time so they can deal with new threats [38].

Prabu et al., (2024), present an innovative NIDS powered by AI that improves performance while resolving data imbalance. For zero-day attack detection, suggest an autoencoder that combines deep and simple architectural implementations to achieve high recall while minimizing false negatives. Evaluate model's performance against industry-standard methodologies to ensure its efficacy [39].

Deldar and Abadi, (2024) DL methods for identifying and categorizing zero-day malware. Research leads us to suggest a taxonomy that classifies various deep malware detection and classification methods that are immune to zero-day attacks into four broad groups: unsupervised, semi-supervised, few-shot, and adversarial resistance. DL architecture, feature encoding, platform, detection or classification capabilities, and whether the authors have completed a zero-day evaluation are some of the criteria that are examined when looking at the methodologies in each area. In addition to discussing the essential features and difficulties of the examined articles, they offer a brief assessment of them [40].

Arun, Nair and Sreedevi, (2024) use LSTM algorithms, notable for their proficiency in gathering correlations among data over time. Cybersecurity is undergoing a paradigm change due to this innovative approach. An elaborate architecture to simulate zero-day attacks, which mimic vulnerabilities that have not yet been found, is developed as the first step of the project. Recurrent neural networks and advanced gating techniques are utilized by LSTM-based detection system. Serious testing proved its ability to detect new attack patterns and identify small deviations from the norm. The end product is an enhanced zero-day attack detection system that is both accurate and quick to react. Because of this, the harm that may be caused by vulnerabilities that are not yet discovered is decreased [3].

Peppes et al., (2023) detail a comprehensive approach that begins with creating realistic zero-day data in tabular form and ends with testing a Neural Network zero-day attack detector trained with and without synthetic data. A fresh and larger dataset of zero-day attack data is synthetically generated through the creation and deployment of Generative Adversarial Networks (GANs). Next, a Neural Network classifier for zero-day assaults is trained and evaluated using the freshly produced dataset from the Zero-Day GAN (ZDGAN). After around 5,000 repetitions, the results demonstrate that the tabular structure for generating zero-day assault data approaches an equilibrium, yielding data that is nearly indistinguishable from the initial data samples [41].

Tran et al. (2022) offer a distributed training method for the online assault detection DL model that protects user privacy. While protecting the confidentiality of local data and parameters, the model enables the sharing of training data to enhance the deep model's accuracy in detecting online attacks. To provide differential privacy, the model employs the method of noise injection into the common parameter [42].

TABLE II. COMPARATIVE EVALUATION OF STATE-OF-THE-ART ZERO-DAY ATTACK DETECTION APPROACHES

Author	Focus	Techniques	Contribution	Identified Limitation
Cherng En et al. (2026)	Cloud-native intrusion detection	Hybrid CNN-LSTM, Kubernetes microservices, SOAR	Developed a scalable AI-enabled intrusion detection framework with improved detection accuracy and automated response.	Limited discussion on explainability, resource utilization, and real-world deployment.
Malkawi & Alhajj (2026)	AI-driven vulnerability management	Systematic review, Deep Learning, LLMs, Deep Reinforcement Learning, Neuro-symbolic AI	Reviewed the evolution of AI-based vulnerability detection and mitigation using PRISMA methodology.	No experimental implementation or comparative performance validation.

Manjula & Saravanakumar (2025)	Zero-day attack detection in cloud security	Machine Learning, Deep Learning, Anomaly Detection, Hybrid Models	Identified the importance of feature engineering, continuous learning, and hybrid AI techniques for zero-day detection.	High false positives, limited interpretability, and dependence on large datasets.
Prabu et al. (2024)	Network intrusion detection	Autoencoder-based Deep Learning	Proposed an AI-based NIDS capable of handling data imbalance while improving zero-day attack detection.	Evaluated on limited datasets with insufficient validation on real-world attacks.
Deldar & Abadi (2024)	Zero-day malware detection	Unsupervised, Semi-supervised, Few-shot, Adversarial-resistant Deep Learning	Presented a comprehensive taxonomy of deep learning methods for zero-day malware detection and classification.	Focuses on classification of existing methods rather than proposing a new detection framework.
Arun, Nair & Sreedevi (2024)	Detection of unknown cyberattacks	LSTM-based Recurrent Neural Network	Utilized temporal learning to detect previously unseen attack patterns with improved detection capability.	Computationally intensive and dependent on sequential training data quality.
Peppes et al. (2023)	Synthetic zero-day data generation	GAN (ZDGAN), Neural Network	Generated realistic synthetic zero-day attack samples to improve neural network performance.	Synthetic data may not fully represent complex real-world attack scenarios.
Tran et al. (2022)	Privacy-preserving web attack detection	Federated Deep Learning, Differential Privacy	Proposed a distributed training framework that preserves data privacy while improving attack detection.	Differential privacy introduces accuracy trade-offs and additional communication overhead.

Research gap: Despite significant progress in AI-driven zero-day attack detection, several research challenges remain unresolved. As summarized in Table II, most existing studies focus on improving detection accuracy using DL, hybrid models, or synthetic data generation, while comparatively less attention is given to model explainability, real-time deployment, and robustness against evolving attack patterns. Moreover, many approaches rely on limited datasets or lack comprehensive validation across diverse cyberattack scenarios, reducing their practical applicability. Privacy-preserving and cloud-native solutions have also received limited experimental evaluation, and the trade-off between detection performance, computational efficiency, and scalability remains insufficiently explored. These research gaps highlight the need for an interpretable, scalable, and robust AI-based framework capable of accurately detecting emerging zero-day attacks in dynamic cybersecurity environments.

7. Conclusion and Future Work

Proactive cybersecurity is essential for cloud computing settings due to the rising sophistication and frequency of zero-day attacks. This review demonstrates that Artificial Intelligence has become a key enabler for detecting unknown threats by learning complex attack patterns that conventional signature-based security mechanisms often fail to identify. Recent advances in ML, DL, hybrid AI models, generative AI, and privacy-preserving techniques have significantly enhanced the capability of security systems to detect and respond to emerging cyber threats. However, the literature also reveals that no single AI technique can effectively address all challenges associated with zero-day vulnerabilities because of the dynamic and evolving nature of modern cyberattacks.

Research in the future should focus on building AI systems that are resilient, adaptable, and easy to understand so that they can run well in massive cloud environments. Greater attention should also be given to benchmarking models on diverse real-world datasets, improving interoperability with cloud-native security platforms, reducing computational complexity, and ensuring compliance with privacy and regulatory requirements.

REFERENCES

1. F. Khoda Parast, C. Sindhav, S. Nikam, H. Izadi Yekta, K. B. Kent, and S. Hakak, "Cloud computing security: A survey of service-based models," Comput. Secur., vol. 114, p. 102580, Mar. 2022, doi: 10.1016/j.cose.2021.102580.
2. S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in 2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

3. A. Arun, A. S. Nair, and A. G. Sreedevi, "Zero Day Attack Detection and Simulation through Deep Learning Techniques," in 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, Jan. 2024, pp. 852–857. doi: 10.1109/Confluence60223.2024.10463429.

4. Y. Guo, "A review of Machine Learning-based zero-day attack detection: Challenges and future directions," 2023. doi: 10.1016/j.comcom.2022.11.001.

5. R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Inf. Fusion, vol. 97, p. 101804, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.

6. S. Kumar, M. Dwivedi, M. Kumar, and S. S. Gill, "A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services," Comput. Sci. Rev., vol. 53, no. C, Aug. 2024, doi: 10.1016/j.cosrev.2024.100661.

7. A. A. Soni, M. Parikh, R. N. K. Dhenia, J. A. Soni, A. R. Jha, and S. M. Shah, "Reinforcement Learning for Dynamic Workflow Optimization in CI/CD Pipelines," in 2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, Dec. 2025, pp. 638–644. doi: 10.1109/CICN67655.2025.11367872.

8. V. K. Sharma, "Cloud Computing IoT: 5G Focused IoT with Cloud Solutions," Int. J. AI, Big Data, Comput. Manag. Stud., vol. 6, no. 3, 2025, doi: 10.63282/3050-9416.IJAIBDCMS-V6I3P103.

9. Y. Muni, "Understanding The Evolution Of Internet Protocols: An In-Depth Review Of Ipv4 And Ipv6: A Comparative Review Of Transition Challenges And Solutions," Int. J. Adv. Res. Comput. Sci., vol. 16, no. 4, pp. 109–117, Aug. 2025, doi: 10.26483/ijarcs.v16i4.7307.

10. E. Hashmi, M. M. Yamin, and S. Y. Yayilgan, "Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security," AI Ethics, vol. 5, no. 3, pp. 1911–1929, Jun. 2025, doi: 10.1007/s43681-024-00529-z.

11. L. Bilge and T. Dumitras, "Before we knew it: An empirical study of zero-day attacks in the real world," in Proceedings of the ACM Conference on Computer and Communications Security, 2012. doi: 10.1145/2382196.2382284.

12. A. Armijos and E. Cuenca, "Zero-day attacks: review of the methods used based on intrusion detection and prevention systems," in 1st IEEE Colombian Caribbean Conference, C3 2023, 2023. doi: 10.1109/C358072.2023.10436218.

13. J. B. Mehta, "Autonomous Patch Validation For Zero-Day Exploits In Enterprise Clouds," Int. J. Appl. Math., vol. 38, no. 4s, pp. 1270–1285, Oct. 2025, doi: 10.12732/ijam.v38i4s.685.

14. S. Singamsetty, "AI-powered Satellite Image Processing for Global Air Traffic Surveillance Techniques Using NCNN–EGSA Optimization Techniques," in Machine Learning Based Air Traffic Surveillance System Using Image Processing, Emerald Publishing Limited, 2026, pp. 179–197. doi: 10.1108/978-1-80592-062-520251010.

15. S. Gupta, "Artificial Intelligence in Cyber Threat Detection: A Survey of Predictive Security Systems," vol. 4, pp. 19–34, 2025.

16. A. Waheed, B. Seegolam, M. F. Jowaheer, C. L. X. Sze, E. T. F. Hua, and S. R. Sindiramutty, "Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure," Jul. 2024. doi: 10.20944/preprints202407.2338.v1.

17. S. F. Ahmed et al., "Deep learning modeling techniques: current progress, applications, advantages, and challenges," Artif. Intell. Rev., vol. 56, no. 11, pp. 13521–13617, Nov. 2023, doi: 10.1007/s10462-023-10466-8.

18. M. H. Hamza Afzal, "Securing AI Systems Against Adversarial Attacks: A Framework for Building Robust and Trustworthy Machine Learning Models," Comput. Fraud Secur., no. 5, pp. 65–74, May 2024, doi: 10.52710/cfs.867.

19. D. Paul, S. A. Devanira Poovaiah, B. Nurullayeva, A. Kishore, V. S. Kumar Tankani, and S. Meylikulov, "SHO-Xception: An Optimized Deep Learning Framework for Intelligent Intrusion Detection in Network Environments," in 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3), IEEE, Jul. 2025, pp. 1–6. doi: 10.1109/ISAC364032.2025.11156610.

20. Y. Roumani, "Patching zero-day vulnerabilities: an empirical analysis," J. Cybersecurity, vol. 7, no. 1, Nov. 2021, doi: 10.1093/cybsec/tyab023.

21. A. Sharma and U. K. Singh, "Cloud Computing Security Through Detection & Mitigation of Zero-Day Attack Using Machine Learning Techniques," in Natural Language Processing for Software Engineering, Wiley, 2025, pp. 357–388. doi:

10.1002/9781394272464.ch25.

22. M. Ahmadi, M. Chizari, M. Eslami, M. J. Golkar, and M. Vali, "Access control and user authentication concerns in cloud computing environments," in 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), IEEE, May 2015, pp. 39–43. doi: 10.1109/TAFGEN.2015.7289572.

23. S. V, G. V, S. G, N. S. P, and S. K, "Ransomware Detection and Prevention," in 2025 6th International Conference for Emerging Technology (INCET), IEEE, May 2025, pp. 1–8. doi: 10.1109/INCET64471.2025.11140093.

24. [24] H. Abusaimeh, "Distributed Denial of Service Attacks in Cloud Computing," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 6, 2020, doi: 10.14569/IJACSA.2020.0110621.

25. S. Kanungo, "Data Privacy and Compliance Issues in Cloud Computing: Legal and Regulatory Perspectives," Int. J. ofINTELLIGENT Syst. Appl. Eng., pp. 1721–1734, 2024.

26. N. Ahmad, "The Structural Modeling of Significant Factors for Sustainable Cloud Migration," Int. J. Intell. Eng. Syst., vol. 14, no. 2, pp. 1–10, Apr. 2021, doi: 10.22266/ijies2021.0430.01.

27. S. Mohamed, S. Kamal, and S. Mostafa, "Advanced Persistent Threats: Detection and Mitigation," 2024, doi: 10.5281/zenodo.20066260.

28. R. Kaur and M. Singh, "A survey on zero-day polymorphic worm detection techniques," IEEE Commun. Surv. Tutorials, 2014, doi: 10.1109/SURV.2014.022714.00160.

29. [29] J. B. Mehta, "Securing Test Automation in Zero Trust Architectures: A Framework for Continuous Verification," in 2025 International Conference on Computer and Applications (ICCA), IEEE, Dec. 2025, pp. 1–5. doi: 10.1109/ICCA66035.2025.11430950.

30. N. Adik, "The Rise of Open and Free Networks: A Community-Driven Paradigm for Decentralized Connectivity," in 2025 IEEE First International Conference on Innovations in Engineering and Next-Generation Technologies for Sustainability (ICINVENTS), Coimbatore, India: IEEE, 2025, pp. 1–9, November. doi: 10.1109/ICINVENTS64613.2025.11402224.

31. R. Zaib and K. Q. Zhou, "Zero-Day Vulnerabilities: Unveiling the Threat Landscape in Network Security," Mesopotamian J. CyberSecurity, 2022, doi: 10.58496/MJCS/2022/007.

32. P Archana, S Kumaravel, and K Gayathri Devi, "Artificial Intelligence–Based Zero-Day Attack Detection and Proactive Mitigation Strategies: A Literature Review," Int. Res. J. Adv. Eng. Hub, vol. 4, no. 02, pp. 474–480, Feb. 2026, doi: 10.47392/IRJAEH.2026.0064.

33. D. Mirza and J. Hudson, "Emerging Cybersecurity Threats and the Role of Artificial Intelligence in Modern Organizations," 2022. doi: 10.13140/RG.2.2.10500.64640.

34. S. Irfan, "Enhancing Email Security Through Accurate Phishing Detection Using Deep Transformer Models," in 2026 World Conference on Computational Science and Technology (WcCST), 2026, pp. 239–244. doi: 10.1109/WcCST67302.2026.11495864.

35. L. Hasimi, D. Zavantis, E. Shakshuki, and A. Yasar, "Cloud Computing Security and Deep Learning: An ANN approach," Procedia Comput. Sci., vol. 231, pp. 40–47, 2024, doi: 10.1016/j.procs.2023.12.155.

36. L. D. Cherng En, A. Alleessa Angelly, S. S. Qistina, N. Kumar Puppala, N. B. Nagaram, and N. Chawla, "Next-Generation Cloud-Native Cyber Defense Using Deep Learning Techniques," in 2026 Innovations in Machine, Engineering, and Digital Conference (IMED), IEEE, Mar. 2026, pp. 1–6. doi: 10.1109/IMED68921.2026.11484443.

37. M. Malkawi and R. Alhajj, "AI-Powered Vulnerability Detection and Patch Management in Cybersecurity: A Systematic Review of Techniques, Challenges, and Emerging Trends," Mach. Learn. Knowl. Extr., vol. 8, no. 1, p. 19, Jan. 2026, doi: 10.3390/make8010019.

38. L. Manjula and E. Saravanakumar, "Zero-Day Attack Detection in Cloud Security: A Survey of Machine Learning and Deep Learning Approaches," in 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), IEEE, Aug. 2025, pp. 2055–2062. doi: 10.1109/ICSCDS65426.2025.11166929.

39. K. Prabu, V. A, R. Radhakrishnan, R. P, E. Thenmozhi, and S. P. Ramesh, "Enhancing Cloud Security with AI-Driven Anomaly Detection for Zero-Day Threats," in 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), 2024, pp. 1087–1092. doi: 10.1109/ICAC2N63387.2024.10895696.

40. F. Deldar and M. Abadi, "Deep Learning for Zero-day Malware Detection and Classification: A Survey," ACM Comput. Surv., 2024, doi: 10.1145/3605775.

41. N. Peppes, T. Alexakis, E. Adamopoulou, and K. Demestichas, "The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers," Sensors, 2023, doi: 10.3390/s23020900.

42. A.-T. Tran, T. D. Luong, X. S. Pham, and T. L. Tran, "Deep Models with Differential Privacy for Distributed Web Attack Detection," in 2022 14th International Conference on Knowledge and Systems Engineering (KSE), IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/KSE56063.2022.9953788.