International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

DETECTING CYBER SECURITY THREATS ON CLOUD COMPUTING NETWORKS OF INTELLIGENT COMPUTING

M.R. Christhu Raj[1], V. Saidulu[2], T.Padmapriya[3], S.V.Manikanthan[4], R.Priya[5]

[1]Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, India

[2]Senior Assistant Professor, Department of Electronics and Communication Engineering, Mahatma Gandhi Institute of Technology, Jawaharlal Nehru Technological University, Hyderabad, India

[3]Melange Publications, Puducherry, India

[4]Melange Academic Research Associates, Puducherry, India

[5]Assistant Professor, Department of AI&DS, Panimalar Engineering College, Poonamallee, Chennai-600123

E-mail: christhm1@srmist.edu.in[1], vsaidulu_ece@mgit.ac.in[2], padmapriyaa85@ptuniv.edu.in[3], prof.manikanthan@gmail.com[4], priyasrp@gmail.com[5]

Abstract

Cloud computing (CC) has gained popularity across a number of industries because of its intrinsic qualities, including scalability and adaptability. But even with these benefits, cloud providers continue to face serious security challenges. Insider attacks, data breaches, and illegal access are among the new vulnerabilities brought about by CC. Attackers are drawn to cloud systems because of their common infrastructure. Society is becoming increasingly reliant on complex and connected cyber systems to carry out everyday tasks. The current study recommends a new cyber security reference model for the cloud system, which consists of separate cloud computing layers. The virtualization and service layers, as well as the crucial elements for ensuring cloud computing safety, are not thoroughly covered by the reference models of cloud computing security that are currently available. Additionally, the social media IoT sensor layer, which gathers messages typed by attackers to launch cyberattacks on the infrastructure of the cloud, and the cyber resilience issues of cloud computing are not taken into account. In order to provide cloud system security, this article also explores the cyber security issues with models of cloud computing and creates an attack framework. Additionally, the integration of threat intelligence systems powered by artificial intelligence (AI) allows for comprehensive understanding of the cyber threat landscape, promoting proactive mitigation strategies and well-informed decision-making to safeguard critical assets and infrastructure in cloud environments. As businesses navigate the dynamic and complex world of cybersecurity, using AI for proactive threat identification is a crucial strategy for bolstering defenses and lowering risks in CC ecosystems.

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Keywords: Artificial Intelligence Algorithms, Cyber Attacks, Cyber Security, Cyber Threat, Detection in Cloud security.

1. Introduction

Cloud computing has significantly changed digital infrastructure, making scalable, personalized computing possible. Its dispersed nature, however, creates additional security risks since attacks are ever more complex and flexible [1]. Traditional systems stumble with real-time responses and are unable to identify zero-day attacks because they rely on pattern matching and predetermined criteria. The requirement for intelligent and flexible defenses is one of the core issues with cloud security. Traditional methods frequently fall short in handling the complex, multi-source data gathered in cloud environments, lack real-time detection capabilities, and are unable to detect innovative attack patterns. A paradigm change toward AI-driven security solutions is necessary to address these issues.

In this kind of cloud assault, destructive activities are carried out by a group of infected computers that hackers control collectively [2]. In order to spread, botnets actively seek a list of IP addresses to search for susceptible PCs or computer networks. Botnets pose a severe threat to user networks, companies and shoppers. Botnets take advantage of today's sophisticated cloud computing platforms and can use a user's network to carry out nefarious tasks like phishing, advertising, distributed disruption of service (DDoS), and data theft. Additionally, a bot acquire can create botnets via cloud services. Bot-cloud, another name for cloud-based botnets, can go up in a matter of minutes and work uninterrupted. One of the most harmful attacks for the victim is when attackers employ malware networks to launch attacks that are hard to stop or even identify. A visual representation of the malware attack is shown in Figure 1. Since there are many botnets on the cloud these days, protection is crucial yet challenging. Botnets are constantly changing to exploit security holes and weaknesses.

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

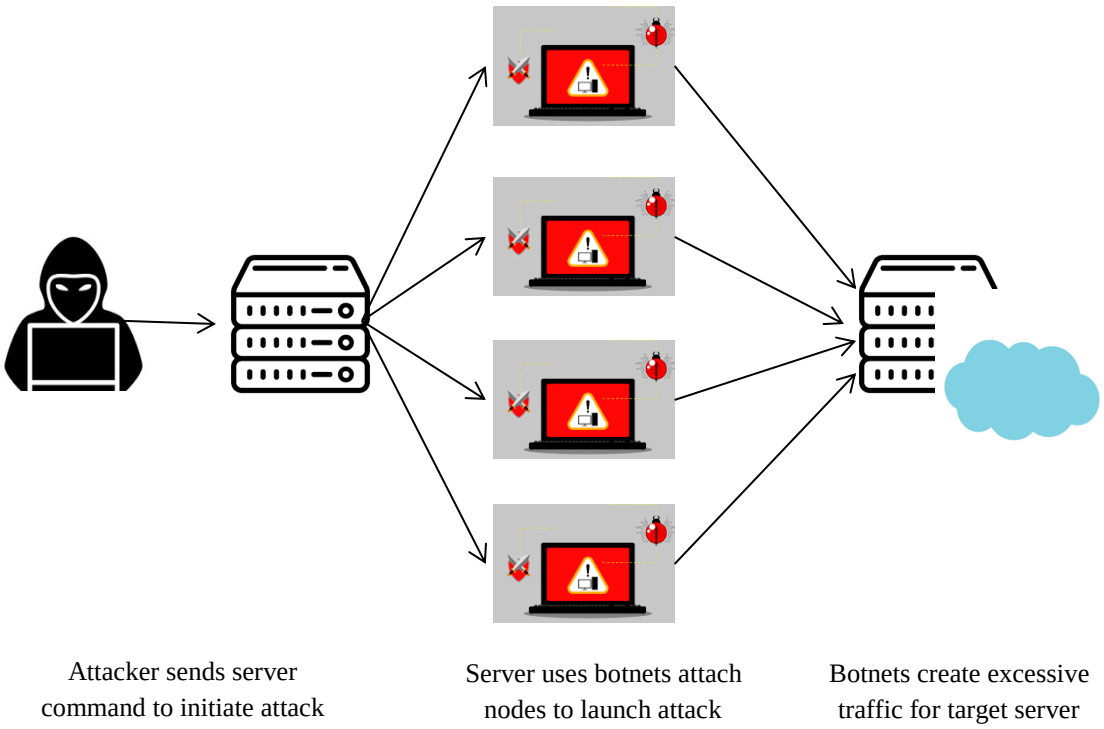

Figure 1. An illustration of a botnet assault

Because it enables efficient data storage, access, and analysis, cloud computing has been adopted by modern enterprises as an essential component. Nevertheless, ongoing cloud technology adoption also raises data security issues. Because they store enormous amounts of sensitive data on cloud servers, including customer information, banking information, and creative work, enterprises are especially susceptible to cyberattacks. Therefore, cloud computing security needs to be enhanced to shield private information from theft and unauthorized access. One possible technique for improving cloud computing security is machine learning (See Figure 2). To find possible security risks, many algorithms can analyze large data sets and learn from the data. Industries can lower the risk of data breaches and improve security procedures by utilizing machine learning.

The cloud package providers are responsible for maintaining the physical facilities which includes servers, drives, and network devices. Therefore, trust between the customer and the cloud service provider is essential to guaranteeing the security of the data stored on cloud servers. The intricacy of the system presents another difficulty for cloud security. Multiple layers of networking, software, and hardware components are present in cloud settings, which make it challenging to recognize and resolve security issues. Because of its cost-saving advantages, scalability, and flexibility, cloud computing has grown in popularity [3]. It does, however, also have a number of flaws that could jeopardize the integrity and security of apps and data.

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

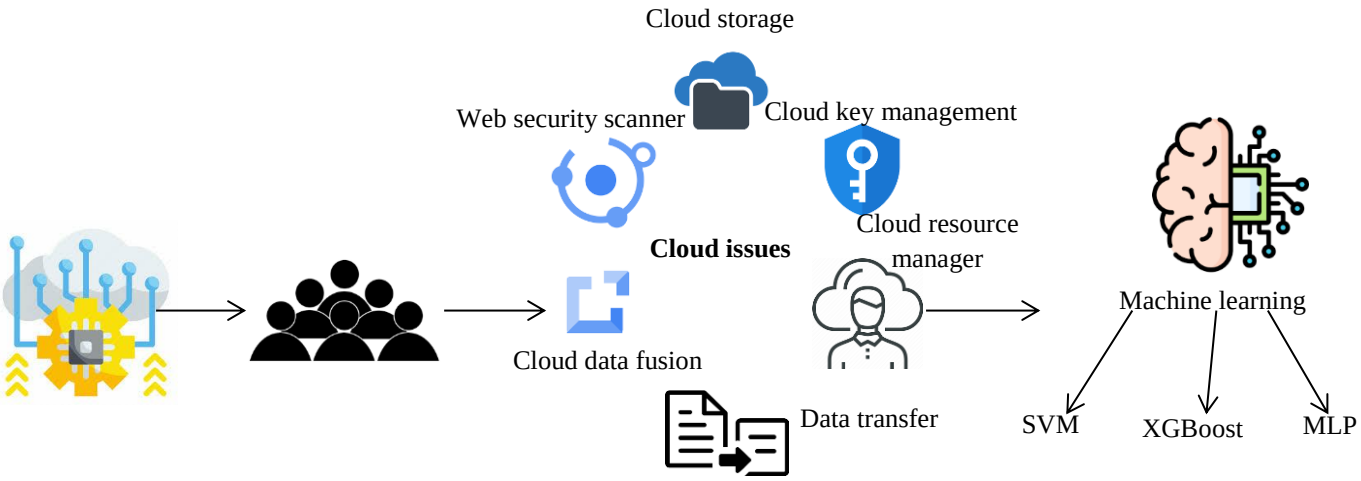

Figure 2. Cloud systems

Employees or authorized users who have access to secured cloud resources are considered insider threats. Cloud systems are susceptible to malware assaults, which include ransomware, worms, and viruses. By flooding the cloud architecture or apps with too many requests or traffic, denial-of-service attacks seek to deteriorate cloud services. Cloud services built on a shared foundation, in which numerous users and apps use the same physical resources, give rise to shared infrastructure hazards.

ML algorithms are employed to improve data management and address security concerns [4]. Machine learning is the use of computational intelligence that enables systems to learn and grow on their own without the need for special modification. The development of applications that can choose an appropriate pace and utilize it to learn independently is the main emphasis of machine learning. In order to find patterns in the information and make better decisions over time, the learning strategy begins with impressions or facts, such as designs, direct knowledge, or heading.

This is how the remainder of the paper is structured. The relevant survey articles are discussed and contrasted with our review work in Section 2. An overview of ML algorithms and a background examination of CC models, risks, and attacks are provided in Section 3 Examines machine learning methods for CC security as well as the goals, methods, benefits, and drawbacks of each research covered in this part 4. In Section 5, we also outline future research directions that should be investigated. In Section 5, the paper is ultimately ended.

2. Related Works

CC is now available as a collection of private and public cloud services, providing customers with a consistent platform across the Internet. IaaS, PaaS, and SaaS are the three primary service paradigms that make up the CC ecosystem. These models are used in community, private, hybrid, and public cloud setups and constitute the core elements of CC. To satisfy the needs of different users, each service model has unique features [5]. By offering virtualization, the foundational layer, Platform as a Service, provides customers with an adaptable and scalable platform to create and manage apps, storage, server hardware, and

Received: August 11, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

network resources. SaaS, on the other hand, provides fully working software programs that customers may access through the cloud, eliminating the need for local installations.

Usually controlled by a single enterprise, this kind of cloud was developed especially to satisfy the company's needs. Private cloud storage can help organizations handle their data more effectively [6]. There are two options: internal leadership and storage or third Company. The material may also contain medical records, trade secrets, and other protected information. The same business owns and operates the infrastructure. Private cloud solutions either use or control the technology, or the architecture/cloud service provider provides the necessary service. Security is more important in private cloud systems than in traditional cloud setups. Compared to a shared cloud, it is easier to control security-related issues and recognize users and suppliers. The advantages of utilizing a private cloud include enhanced security and privacy, cost and energy economy, and greater monitoring. There are disadvantages to using a private cloud, including fixed pricing and less scalability due to resource limitations.

Following an examination of their possible attributes, conventions were used to construct new factual stream highlights. The next step was the creation of an AdaBoost group instruction method that used three AI approaches to evaluate the influence of these parameters and differentiate between damaging events [7]. It was determined through correlation and correlation coefficient assessments that the suggested highlights might show either beneficial or detrimental activity. Furthermore, the suggested collecting strategy demonstrated a reduced percentage of false positives and a greater recognition rate in comparison to the algorithm and three other best-in-class grouping methods. Using the IoT/Fog/Cloud standards, miniature authorities, and DevOps foundations, the reference engineering, model execution, and city scale contextualized inquiry assessment of PROMENADE—a stage that ensured perpetual enhancement of powerful alongside solid uses for ongoing checking and inspection of roadway data produced by IoT devices in massive intelligent urban areas areas—were gave.

Finding, controlling, and reducing security threats related to cloud infrastructure is the primary goal of CSPM. It accomplishes this by automatically checking and evaluating cloud resources for errors, settings, and compliance infractions that can put a company at risk for security breaches. CSPM products give enterprises insight into the infrastructure as cloud environments grow more complicated and scalable [8]; assisting them in making sure they comply with security regulations, industry best practices, and legal requirements. These technologies assist businesses in avoiding possible threats that can jeopardize the honesty of the cloud environment and in consistently maintaining a solid security posture.

Using a service-oriented construction, the authors of other recent works [9] examine the cyber threat landscape with a focus on the threat modeling phase of system defense and attack. The study suggests that users should take on a portion of the duty to take into account potential attackers and attack paths, which is often the responsibility of the internet service provider (ISP). The four main features of cloud services are handling data, information transfer, data storage, and cybersecurity. These four traits serve as the basis for analyzing a small number of cloud service-related issues in the conventional method of cyber threat identification. Despite its usefulness, the authors claim that this method does not fully analyze the entire computing ecosystem.

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Threat detection capabilities in cloud systems have been transformed by recent developments in deep learning architectures. CNN-based methods have shown to be successful in analyzing network traffic. Using deep learning, Qin et al. created a segmentation-based authentication system that was very accurate in differentiating between malicious and valid access patterns [10]. Expanding upon this work, a CNN-RNN hybrid technique laid the groundwork for multi-dimensional security analysis by utilizing both spatial and temporal data to enhance authentication. One especially effective method for security monitoring is the combination of convolutional models with LSTM networks. It has been shown that CNN-LSTM combination models perform better than conventional machine learning techniques because LSTMs are excellent at identifying long-term relationships in sequential statistics, which makes them perfect for examining network traffic trends that change over time.

3. Methods and Materials

3.1. The importance of artificial intelligence-infused clouds security threat detection and incident reaction

Organizations must use cutting-edge security measures to protect sensitive data hosted on the cloud as cyber threats increase [11]. AI improves the speed and accuracy of event reactions. In order to reduce the consequences of security breaches, prompt response is crucial. AI automation reduces turnaround times and the requirement for manual intervention by ensuring timely actions [12]. Therefore, in order to reduce the damage caused by security events, organizations that wish to stay ahead of these threats need understand how to strategically integrate cloud security with AI operations.

This article acknowledges the continuous and pressing need for strong security measures for the specially tailored cloud architecture in order to help organizations create effective and targeted security programs.

3.2. The application of AI to threat recognition

Maintaining a strong defense versus cyberattacks requires an understanding of potential dangers in cloud security [13]. By leveraging AI's sophisticated capabilities, which outperform traditional methods, businesses can increase their security.

AI makes proactive detection of risks in cloud security possible in this way.

3.2.1. Anomaly uncovering

AI schemes are a crucial line of defense against zero-day assaults in anomaly detection because of their exceptional ability to identify deviations from the norm. The establishment of norms, a dynamic process that enables AI perpetually observe and learn from the complex network of system and user activity taking place in a cloud environment is the basis of this approach.

The first step in empowering AI to identify abnormalities is to establish appropriate baselines that incorporate common cloud ecosystem operations. AI can identify typical interactions and instances across buildings, apps [14], and people through ongoing sensing

Received: August 11, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and training. The short ID of aberrations that can suggest potential security risks is used in conjunction with a comprehensive perspective. Furthermore [15], AI systems may adapt and enhance their understanding of normality as user behaviors, network behavior, and system operations are continuously analyzed, ensuring that beginnings will remain relevant even when user habits and system settings change. AI grows skilled at promptly recognizing anomalies, or the sudden departures from learnt norms, once standards have been set. Understand that anomalies can manifest in a variety of ways, such as odd data transfers or inconsistent access practices.

3.2.2. Behavioral analytics

To strengthen surveillance and behavioral analytics defenses against insider threats, AI can recognize and assess dubious behavior. This approach depends on AI's capacity to comprehend typical user behavior and rigorously detects deviations from predetermined standards. AI easily combines cloud security and behavioral analytics through User and Entity Behavior Analysis (UEBA) [16]. AI is skilled at identifying unusual activity by precisely assessing the behaviors and actions of people and things in cloud environments. For example, AI could provide a proactive protection against unwanted access by detecting whether a user is attempting to access confidential information from an unauthorized location. Sorting through the massive amounts of electronic systems and internet information to find anomalies is the main problem in internet safety. As a result of weariness or disinterest, AI systems thrived when concentrating on event data streams.

Cloud security artificial intelligence can detect anomalous activity that suggests compromises or insider threats by building user profiles based on typical behavior. In the current research, geolocation, login timing, downloaded information trends, and available resources are all considered. Furthermore [17], AI can use natural language processing to analyze conversations for signs of potential intimidations.

3.2.3. Automated incident reaction

Intelligent technology speeds up recovery times and minimizes damage by streamlining crisis response procedures [18]. AI may accomplish this by promptly recognizing and addressing threats without the need for human involvement. This feature of safety automation increases the efficacy of situation control while enabling sophisticated and smooth threat detection and response in cloud security. Despite requiring human intervention, AI's rapid threat identification and handling reduces the effect of security incidents. AI can ensure a timely and efficient response to emerging risks by, for example [19], automatically quarantining compromised devices or reversing changes made by cybercriminals.

A variety of repetitive and routine security duties that are prone to human error are also included in security automation. These consist of putting firewalls in place, checking for malware, responding to alerts, addressing vulnerabilities, and updating passwords. When these security jobs are automated with AI, the cyber security teams may concentrate on more important tasks like threat hunting, ongoing monitoring, and enhancing the overall security situation. AI-driven computerization relieves the teams of these tedious tasks, which improves

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

response times and reduces the possibility of mistakes, making the security system more flexible and practical and encouraging continuous security enhancement.

3.2.4. Threat intellect

Through interaction with threat data sources, AI solutions assist enterprises in staying ahead of the always changing danger scenario. Real-time updates are made possible by the integration, guaranteeing that the cloud security architecture is always current with the newest threats. Therefore, AI-enabled safety devices can assist in detecting and responding to potential threats using the most recent information by keeping ahead of malicious intelligence. Consequently, AI techniques are crucial for figuring out the best encryption plans for intricate cloud setups. Due to the global cloud ecosystem's complexity, an efficient encryption technique that consistently balances privacy and efficiency is required.

3.2.5. Tools for cloud-native security

Strong threat detection and incident responses with smooth AI integration are offered by providers. These technologies are crucial parts of improving security measures when they are created specifically for cloud environments. For managing protection across several clouds from different providers, a cloudnative security platform (CNSP) provides a complete solution. An NSP is essential in streamlining cloud-native tracking, disaster recovery, and regulatory operations by developing a safety framework that incorporates best practices relevant to numerous stakeholders.

3.3. Cloud computing systems' service delivery paradigms and cyber security concerns

Three service models are used by cloud computing to offer users a range of services. Customers can access application platforms, software resources, and infrastructure resources as a service through the cloud computing service models known as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). The cloud environment is subject to varying security requirements depending on the service model.

The lowest fundamental tier of the cloud computing service model stack is the Infrastructure as a Service (IaaS) paradigm. At the top layer of the IaaS model is the PaaS model, and at the top layer of the PaaS model is the SaaS model.

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

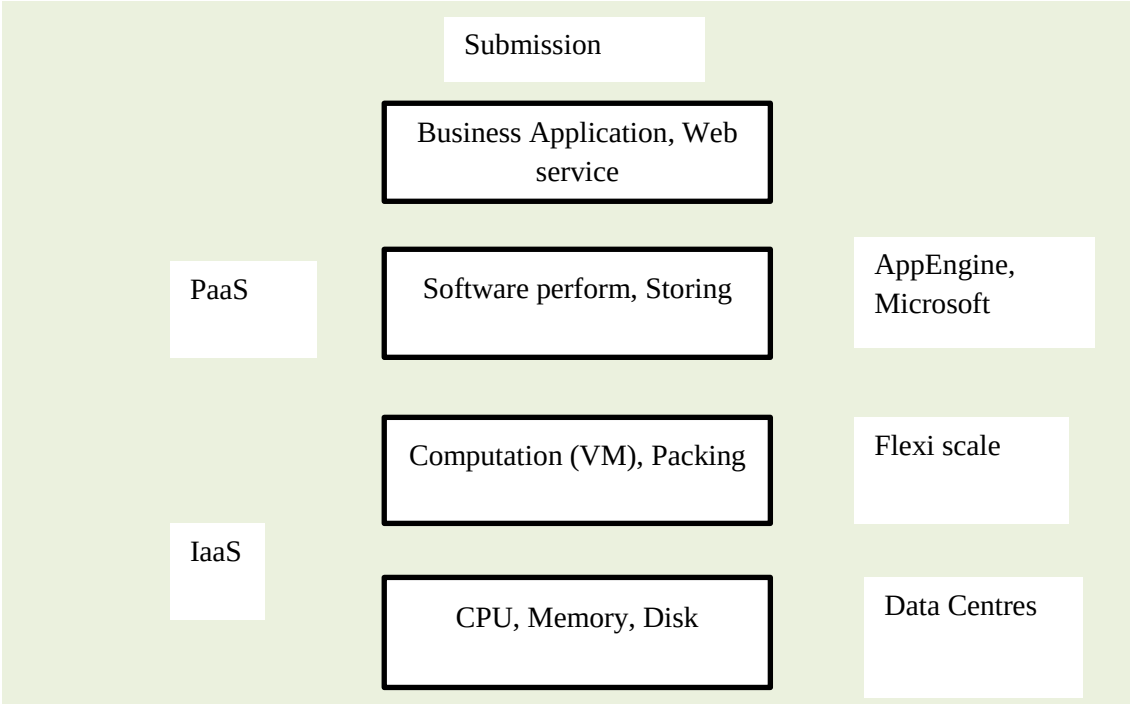

Figure 3. Layered cloud system architecture

Each of these levels is located above the others. Each layer is built with the assumption that the layers that lie beneath it are somewhat connected. This feature in Figure 3 allows each layer to run autonomously.

4. Implementation and Experimental Results

4.1. Dataset

The majority of studies used a variety of publicly available datasets to experimentally validate and assess suggested methodologies, According to state-of-the-art

literature, several people created their datasets for CI-based IDS over CC and MCC.

The researchers looked at cloud computing security from a different angle. Given how quickly clouds are changing in the modern world, security problems and concerns must be identified quickly. While some survey reports have categorized security risks based on people, processes, and technology, others have highlighted issues based on the cloud architecture [20]. Some have addressed security issues generally, while others have only addressed data security and privacy. It is necessary to draw attention to and resolve new security threats in the field of cloud computing. The information from related surveys and studies regarding security concerns in cloud computing is compiled in Table 1.

Table 1. An overview of related assignments

Focus	Key Features and Limitations
The risks to protection and how to mitigate them	• Established security risks and solutions from the standpoint of cloud privacy issues. • Categorized, examined, and resolved the security flaws. • Compare the many risks and assaults that the cloud

Received: August 11, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	environment is subject to.
Problems with cloud security and how to fix them	• Addressed about several aspects of the cloud environment, cloud security problems, cloud dangers, and remedies. • Identified key cloud-related subjects, including infrastructure and framework, services, innovations, deployment approaches, threats and attacks, and cloud security ideas. • Defined unresolved cloud security research questions.
Design and implementation of cloud computing	• Cloud sections, installation simulations, protection of the cloud, and investigated cloud service models were all part of the cloud computing concept. • Identified possible threats and real-world security concerns. • TTP was introduced in order to guarantee security features.
Malware and clouds algorithms	• Examined several cloud models and attributes from a security standpoint. • Carefully investigated cloud security requirements and challenges, and put forth a new approach to mitigate them. • Inquired about cloud security concerns without concentrating on potential future research avenues for IoT-based clouds.

Since 1999, Anomaly detection techniques have been tested on the KDD Cup 1999 dataset. Researchers used the DARPA 1998 data set, which comprises military network breaches, to develop machine learning-based grouping and classification methods with a specific security focus. The training data is more than five million connections records over three weeks from the KDD Cup 1999 dataset. The training data consists of quantitative and statistical variables that are classified as either typical traffic or the type of assaults. Four types of attacks are included in the dataset, which is commonly used for network-based anomaly detection systems: DoS, User-to-Remote, searching, and Remote-to-Local. The KDD Cup 1999 dataset consists of three different feature classes: fundamental features, content features, and traffic characteristics [21]. Every feature related to TCP connections is included in the basic class. Traffic categories are created using features related to a window time period, and the set of functions that analyze the data section's risky behavior then invokes the data elements.

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

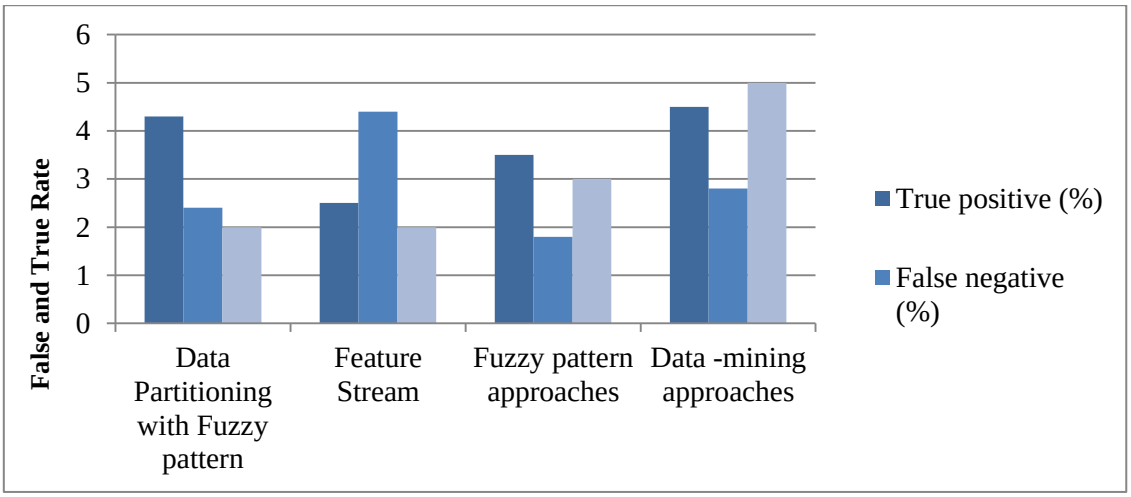

Figure 4. Behavior-based botnet detection methods are compared against relevant baselines

By precisely modifying the fuzzy pattern's membership functions, the authors improved the detection efficiency. The true positive, false negative and false-positive rates are used to assess the results, and they are contrasted with feature flow, fuzzy pattern, static analysis, and data-mining techniques. Figure 4 illustrates how the suggested approach outperforms all baselines taken into consideration, achieving a false-positive alarm rate of less than 4.5% and detecting roughly 85% of bots.

The SVM algorithm is used in this online anomaly-based detection technique to find malware at the cloud's hypervisor level. To generate the feature set and extract the characteristics, the authors in this work used end-system and network-level data. Their approach can identify anomalies with 80% detection accuracy when using system-based data, but its performance is poorer when using network-level features. Nevertheless, their findings demonstrated that the suggested application of the SVM method for malware detection may identify irregularities at the lowest possible time cost.

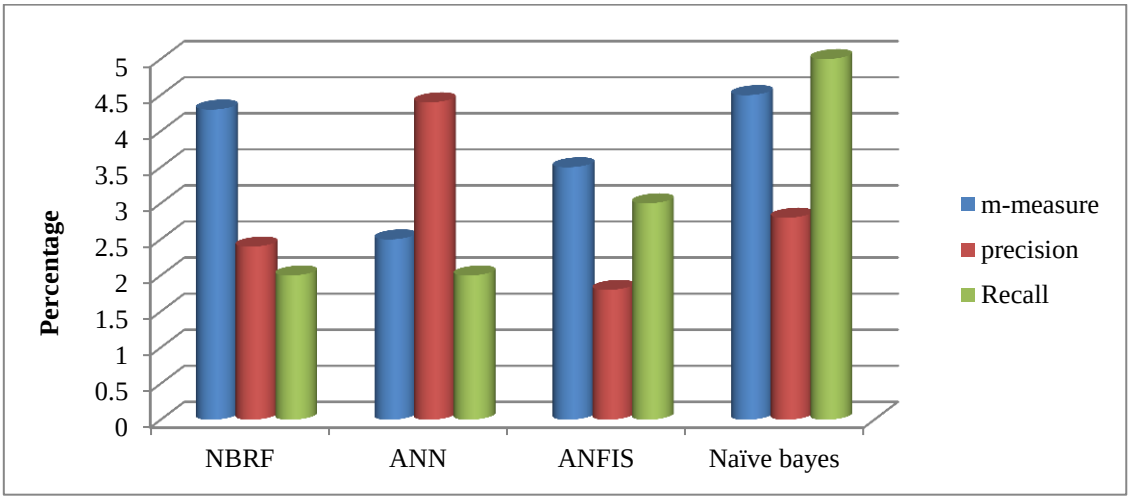

Figure 5. ANFIS's assessment of baseline techniques for detecting attacks on the DARPA KDD Cup dataset

Received: August 11, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Without being installed in the virtual machines directly, this HVI is able to identify both network-based and host-based operations. The authors evaluated the efficacy of ANFIS using five distinct assault scenarios and the DARPA KDD Cup dataset. The outcomes were evaluated using precision, recall, and F-measure scores. Figure 5 displays the outcomes of analyzing ANFIS with ANN, NBRF, and Naïve Bayes for regular relationships. We can observe that ANFIS has a recall that is equivalent to other approaches, but it's precision and F-measure are higher.

The fuzzy C-Means clustering method is called FCM-ANN. This concept eliminates the requirement for manual recording of the attack patterns. It consists of three phases: fuzzy grouping, fuzzy collection, and ANN modules. In the initial stage, the suggested approach divides data into tiny groups to enhance the ANN's capacity for learning. ANN modules are trained using the parameters of the designated clusters in the following phase.

The final aggregation module integrates the ANN's results. The experiment was carried out by the authors using the DARPA KDD Cup dataset. Figure 6 displays the accuracy, recall, and F-measure values obtained by contrasting the proposed model with conventional ANN and Naïve Bayes.

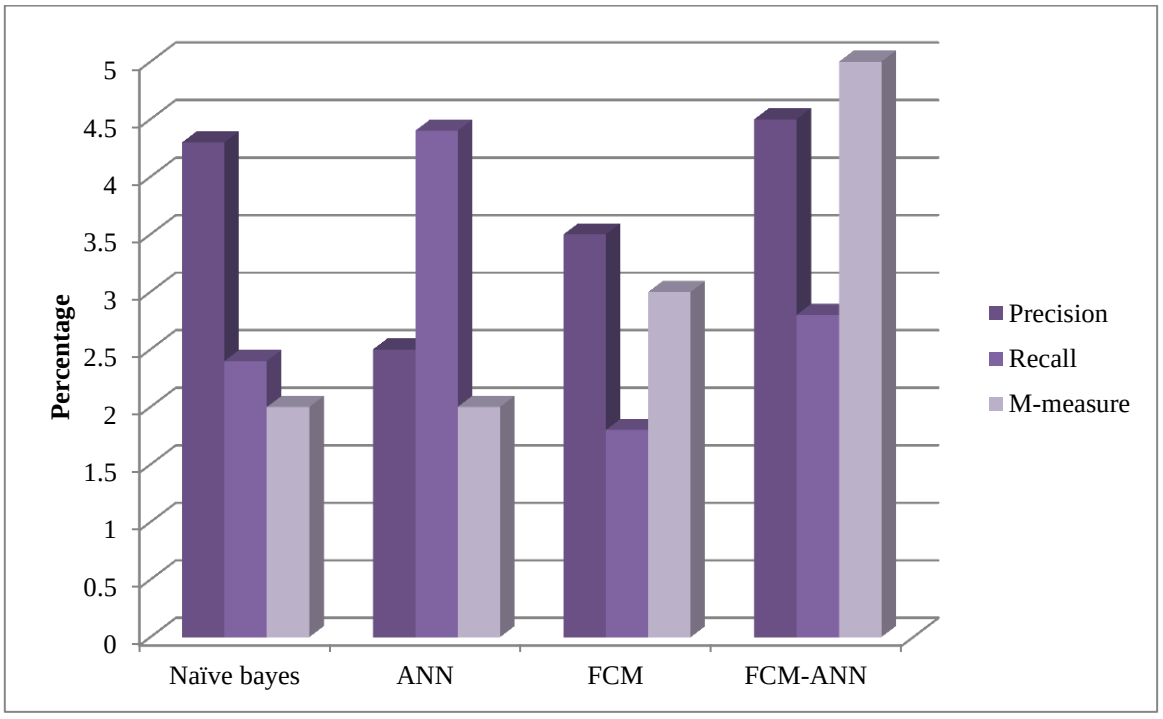

Figure 6. FCM-ANN, Naïve Bayes, and regular ANN performance on the DARPA KDD Cup dataset

The authors employed GA to get over Fuzzy NN's detection rate issues and Distinguish between users-to-root and remote-to-local attacks. They employ a four-level strategy. Employing the k-means method, which is a good option for clustering methods in terms of accuracy, clustering is implemented at the first level. The fuzzy rules are extracted using a GA method in the second level, and the rule base is optimized using this GA in the third level. Lastly, the fuzzy neural network refines the parameters on the fourth level. Following these

Received: August 11, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

stages, the authors developed an intrusion detection rule base a Deep Learning-based system for cyberattack detection and prevention in MCC.

On three publicly available datasets, the proposed method consistently outperforms other machine learning-based approaches in terms of accuracy, precision, and recall; an examination and categorization of MCC intrusion detection techniques within the framework of 5G networks, with a focus on the challenges posed by this scenario. Additionally, they offered a more advanced framework for implementing IDS techniques in mobil cloud-based 5G networks so as to offer secure MCC.

5. Conclusion

Cloud computing has emerged as the foundation of contemporary infrastructure in today's highly interconnected digital environment. However, it is a prominent target for cyber-security risks due to its scattered nature. This talk examined how intelligent computing, which includes automation, machine learning, and AI, can be used to successfully identify and counteract these threats.

Traditional security methods often fall short in these complex, dynamic environments. This is where intelligent computing—which includes AI, ML, and data analytics—plays a vital role. This presentation explores how intelligent computing enhances the detection of cybersecurity threats in cloud networks. By leveraging real-time monitoring, pattern recognition, and automated response capabilities, intelligent systems can significantly improve threat detection and response, ensuring stronger protection for cloud-based infrastructures.

Through our research, we have demonstrated how CI-based IDSs necessitate meticulous parameter adjustment in order to achieve their objective with high accuracy; also, the performance-evaluation criteria used in various studies are not always consistent. Furthermore, there are still insufficient intrusion detection datasets, and the majority of the works rely their assessment on KDD '99 and its variations, which refers to outdated datasets unfit for confirming IDS proposals in cloud environments. Because signature-based techniques necessitate a continuous updating of the knowledge base, which is difficult to get, the variety and dynamicity of CC present an additional challenge.

Additionally, depending on the application, there may be different locations for IDS deployments, which is currently up for debate. Lastly, even though CC and MCC share comparable paradigms, MCC scenarios lack appropriate IDS; in fact, the majority of researchers concentrated on authentication techniques to protect data in MCC. This lack of progress may be caused by the inefficiency of current CC-IDSs for MCC, their lack of datasets, or the lack of current performance criteria to apply in mobile settings. Given these limitations, we argue that more research is needed for CI-based IDS in MCC. Additionally, additional potential directions can be imagined based on our conversation.

References

[1] Y. Wang & X. Yang. Research on enhancing cloud computing network security using artificial intelligence algorithms. “arXiv preprint arXiv” Vol 25 no. (02) pp.17801. 2025.

Received: August 11, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[2] S. Yadav, K. D. Kalaskar, & P. A Dhumane, Comprehensive Survey of IoT-Based Cloud Computing Cyber Security. "Oriental journal of computer science and technology", Vol 15 no. (1, 2, 3), pp.27-52. 2022.

[3] Z. Abbas, & S. Myeong. Enhancing industrial cyber security, focusing on formulating a practical strategy for making predictions through machine learning tools in cloud computing environment. "Electronics", Vol. 12 no. (12), pp.2650. 2023.

[4] U. A. Butt, M. Mehmood, S. B. H. Shah, R. Amin, M. W. Shaukat, S. M. Raz, & M. J. Piran. A review of machine learning algorithms for cloud computing security. "Electronics", Vol 9 no. (9) pp. 1379. 2020.

[5] H. Attou, M. Mohy-eddine, A. Guezzaz, S. Benkirane, M. Azrour, A. Alabdultif, & N. Almusallam. Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. "Applied Sciences", Vol 13 no. (17), pp. 9588. 2023.

[6] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, & Z. Jalil. Cyber security in iot-based cloud computing: A comprehensive survey. "Electronics", Vol 11 no. (1), pp. 16. 2021.

[7] E. M. Onyema, S. Dalal, C. A. T. Romero, B. Seth, P. Young, & M. A. Wajid. Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities. "Journal of Cloud Computing", Vol 11 no. (1), pp. 26. 2022.

[8] E. Bazgir, E. Haque, N. B. Sharif, & M. F. Ahmed. Security aspects in IoT based cloud computing. "World Journal of Advanced Research and Reviews", Vol 20 no. (3), pp. 540-551. 2023.

[9] A. C. Inaganti, N. Ravichandran, S. R. K. Nersu, & R. Muppalaneni. Cloud Security Posture Management (CSPM) with AI: Automating Compliance and Threat Detection. "Artificial Intelligence and Machine Learning Review", Vol 2 no. (4), pp. 8-18. 2021.

[10] V. Chang, L. Golightly, P. Q. A. Modesti, L. M. T. Xu, Doan, K. Hall, & A. Kobusińska. A survey on intrusion detection systems for fog and cloud computing. "Future Internet", Vol 14 no. (3), pp. 89. 2022.

[11] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, & S. J. Abdulkadir. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. "Electronics", Vol 11 no. (2), pp. 198. 2022.

[12] M. Jangjou, & M. K. Sohrabi. A comprehensive survey on security challenges in different network layers in cloud computing. "Archives of Computational Methods in Engineering", Vol 29 no. (6), pp. 3587-3608. 2022

[13] A. R. P. Reddy. The role of artificial intelligence in proactive cyber threat detection in cloud environments. "NeuroQuantology", Vol 19 no. (12), pp. 764-773. 2021/

[14] I. H. Sarker, M. H. Furhad, & R. Nowrozy. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. "SN Computer Science", Vol 2 no. (3), pp. 173. 2021.

[15] A. Salih, S. T. Zeebaree, S. Ameen, A. Alkhyyat, & H. M. Shukur (, February). A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In 2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic"(IEC) pp. 61-66. IEEE. 2021, February.

Received: August 11, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[16] H. Lin, Q. Xue, J. Feng, & D. Bai. “Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine”. Digital Communications and Networks, Vol 9 no. (1), pp. 111-124. 2023.

[17] Z. Tong, F. Ye, M. Yan, H. Liu, & S. Basodi. “A survey on algorithms for intelligent computing and smart city applications”. Big Data Mining and Analytics, Vol 4 no. (3), pp. 155-172. 2021.

[18] S. El Kafhali, I. El Mir, & M. Hanini. “Security threats, defense mechanisms, challenges, and future directions in cloud computing”. Archives of Computational Methods in Engineering, Vol 29 no. (1), pp. 223-246. 2022.

[19] W. S. Admass, Y. Y. Munaye, & A. A. Diro. “Cyber security: State of the art, challenges and future directions”. Cyber Security and Applications, Vol 2, no. 100031. 2024.

[20] N. Tissir, S. El Kafhali, & N. Aboutabit. “Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal”. Journal of Reliable Intelligent Environments, Vol 7 no.(2), pp. 69-84. 2021

[21] S. D. Pasham. “Graph-Based Models for Multi-Tenant Security in Cloud Computing”. International Journal of Modern Computing, Vol 4 no. (1), pp. 1-28. 2021.

Received: August 11, 2025