Research Article

Journal of Contemporary Education Theory & Artificial Intelligence

Towards Proactive Cloud Security: A Survey on ML and Deep Learning-Based Intrusion Detection Systems

Sivaprasad Yerneni Khaga[1], Ravi Teja Avireneni[2], Sri Harsha Koneru[3], Naresh Kiran Kumar Reddy Yelkoti[4]

[1]Infoway Software,O365 Lead Developer, MailSivaYerneni@gmail.com
[2]LACARE ,Lead Weblogic Engineer, ravireneni@gmail.com
[3]Infoway Software,Systems Administrator, Harsha.srihk@gmail.com
[4]U.S. Bank, Sr. Information Security Engineer, reachnareshy@gmail.com

***Corresponding author:** Sivaprasad Yerneni Khaga

IJCACI and Washington University of Science and Technology (WUST) Conference Proceedings 2025
https://scrs.in/conference/ijcaci2025/page/Best%20Paper%20Award

Citation: Sivaprasad Yerneni K, Ravi Teja A, Sri Harsha K, Naresh Kiran Kumar Reddy Y (2025) Towards Proactive Cloud Security: A Survey on ML and Deep Learning-Based Intrusion Detection Systems. J Contemp Edu Theo Artific Intel: JCETAI-116.

Received Date: 05 Sep, 2025; **Accepted Date:** 17 Sep, 2025; **Published Date:** 25 Sep, 2025

Abstract

Cloud storage servers are attractive to individuals and businesses due to the accessibility of their services and the scalability of computing activities. With its scalable, affordable, and on-demand processing resources, cloud computing has rapidly become the standard for data management and service delivery across various industries. However, this paradigm shift has introduced significant security challenges due to its distributed architecture, multi-tenancy, and reliance on web technologies. Traditional Intrusion Detection Systems (IDSs) are increasingly ineffective in such dynamic environments, necessitating more adaptive and intelligent solutions. This overview investigates the role of ML and DL methods in enhancing IDS frameworks hosted in the cloud. As a result of ML, complicated network traffic may be efficiently analyzed for anomalies. The research delves further into cooperative intrusion detection system designs that tackle changing cyber threats by utilising shared intelligence among cloud providers. This study provides a comprehensive overview of how AI-driven intrusion detection systems (IDSs) can enhance intelligent, proactive, and resilient cloud security systems by examining current methods, challenges, and emerging trends.

Keywords: *Cloud computing, intrusion detection system (IDS), machine learning (ML), deep learning (DL), cybersecurity, cloud security threats, IDS, anomaly detection.*

I. Introduction

The phenomenon of cloud computing has radically changed the conventional paradigms of computing, providing individuals and organizations with scalable, on-demand services through the Internet [1]. The move allows application, data, and services to be shifted to distributed facilities, and users reap the benefits of lower local computational overhead and of pay-as-you-go arrangements. This implies that many industries, such as e-commerce, healthcare, education, and banking, are rapidly innovating due to cloud computing, which is crucial to digital transformation [2].

The proliferation of cloud computing, however, has given rise to numerous security concerns. Multiple tenants, shared resources, dynamic provisioning, and diverse traffic all contribute to the dispersed nature of cloud environments, making them more vulnerable to attacks [3]. DDoS attacks, APTs, unauthorized access, and zero-day vulnerabilities are common threats to the confidentiality, availability, and integrity of data and services hosted in the cloud.

Cloud security architectures have now incorporated Intrusion Detection Systems (IDSs) to address these increased security issues.An intrusion detection system is designed to monitor a system or network for any indication of suspicious behavior or policy violations. However, Traditional IDSs are becoming increasingly ineffective in cloud environments because their functionality lacks flexibility and is based on known signatures or predefined rules. The development of cooperative IDSs is based on the consideration that an individual IDS cannot identify all forms of attacks in a highly distributed environment. Agents from various cloud providers collaborate in these systems to enhance detection capabilities by exchanging feedback and insights [4].

Adaptive and intelligent systems for threat detection have recently become available due to advancements in AI, ML, and DL, which have significantly transformed the landscape of intrusion detection [5][6]. The resulting ML algorithms can sort through vast amounts of heterogeneous network traffic and identify patterns that were previously difficult to discern with the limited information produced by a human working alone. An example is that the embedded ML into IoT-based sensors (e.g., smart surveillance cameras) can transmit only the relevant data (or events, e.g., detections of certain objects) to allow further processing to take place, which reduces overhead costs and the time required to respond to it [7].

Additionally, academics are investigating how Deep Learning techniques such as RNNs, LSTMs, CNNs, and Autoencoders can depict complex, non-linear relationships in data with a high degree of dimensionality. Highly effective for cloud-based IDS solutions, these methodologies offer expanded capabilities in feature extraction, anomaly detection, and multi-class classification. The demonstrated efficacy of DL in domains such as computer vision, biological signal analysis, and natural language processing suggests that it may be a valuable asset to an autonomous and proactive cybersecurity architecture.

A. Organisation of the Paper

The paper's structure is as follows: First, we provide some context regarding IDC's Proactive Cloud Security and how it utilizes machine learning. Part II provides an Introduction to Intrusion Detection Systems. Section III outlines the various security threats to cloud computing. Examining IDS's ML and DL capabilities is covered in Part IV. Section V concludes the investigation and lays out the next steps.

II. Overview of Intrusion Detection Systems (IDS)

A Series of security, confidentiality, and privacy issues have been associated with the use of computer systems and the Internet in recent times due to the need to transfer data electronically. Hence, studies have focused on improving privacy and securing computer systems, but despite these efforts, these problems still persist in computer systems, to the extent that there is currently no completely secure system on the planet. Attacks are launched in various forms, emerging in response to the existence of new signatures with abnormal behavior in the signature database [8]. Therefore, several tools have been used to counter different forms of attacks on network systems and one such tool is IDSs shown in Figure 1. This tool was developed for real-time monitoring of network systems for any form of intrusion. They aim to detect attacks that target the system's security features.

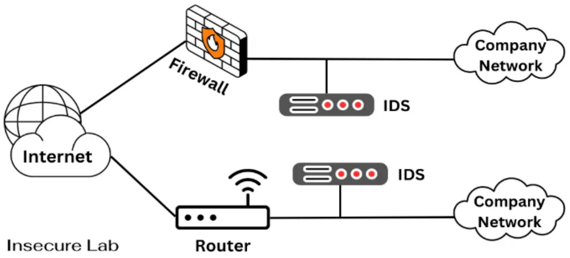

Fig. 1. Intrusion Detection Systems (IDS).

B. Intrusion Detection Detect Network

The use of an IDS is one kind of surveillance. The two most popular types of IDS are host-based and network-based. Intruder detection systems can be either host-based or network-based; however, the former is more narrowly focused on identifying incursions on specific hosts, while the latter searches the entire network for suspicious activity. Monitoring the packets that packet sniffers transmit is one function of network intrusion detection systems. Since NIDS can monitor more network targets, it can detect more attacks that HIDSs may miss, as they cannot view packet headers. For instance, NIDS can detect numerous IP-based DoS attacks because it monitors packet headers as they pass through the network. Furthermore, NIDS relies less on the host operating system as a detection source; instead, it is designed to work effectively with specific operating systems. HIDS and NIDS have been combined in some hybrid IDSs and used to detect intrusions.

C. Techniques for Intrusion Detection Systems

An intrusion detection system can use the following methods:

1) Signature-Based Detection

The signature-based detection method is one type of attack detection that uses patterns of known attacks to identify potential threats. These patterns are obtained from a signature database and compared whenever fresh system activity or network traffic is identified. Whenever the system detects a match, an alarm is set off.

2) Anomaly-Based Detection

An anomaly-based detection system establishes a normal state for a system or network and flags any deviation from this as a potential intrusion. Anomaly detection can identify novel threats, as it is not dependent on known attack patterns, unlike signature-based approaches.

3) Hybrid Detection

Hybrid detection systems attain peak performance by combining signature-based and anomaly-based methods. These systems utilize signature recognition to identify known threats and monitor deviations from normal behaviour, thereby detecting previously unknown attacks. When both methods are used together, the rate of detection increases and the number of false hits decreases.

4) Heuristic and Statistical Techniques

Heuristic and statistical approaches involve defining specific rules or leveraging mathematical models to detect intrusions. For example, a rule may trigger an alert if the number of failed login attempts exceeds a predefined threshold. Similarly, statistical techniques can analyze traffic distributions or compute entropy to identify unusual variations that may indicate an attack. These techniques are well-suited for resource-constrained real-time applications due to their simplicity and computational efficiency.

D. Applications of Intrusion Detection Systems (IDS)

One crucial instrument in cybersecurity for monitoring and detecting intrusion attacks is the Intrusion Detection System (IDS). Intruder detection systems can be categorised into three main types: application, host, and network. Intrusion detection systems scan networks for suspicious packets. Host intrusion detection systems typically monitor only one server or computer. Lastly, application intrusion detection systems monitor several apps known to pose a threat [9][10]. One crucial piece of technology that can protect individuals from cyberattacks is intrusion detection systems (IDS). Due to the prevalence of various forms of cybercrime, the Internet has become the de facto medium for all financial transactions and data processing. Information security must, therefore, get increased focus. This paper covers the following application areas:

- IoT Intrusion Detection System
- Security for Smart Cities
- Intrusion Prevention System for Big Data Systems
- Security System for Fog
- Protection against Mobile Threats.

1) IDS for Internet of Things (IoT)

A network of networked computing devices, goods, and services that can sense, collect, and transfer data over the Internet without any human interaction is called the IoT. Low-power, lightweight protocols are built into Internet of Things devices [11]. In terms of discussions involving smart grids and IoT devices, it is not heavy. The system is highly susceptible to attacks, as they can manipulate the data gathered by the sensors. The majority of assaults on IoT devices fall into one of several categories: physical, side channel, environmental, cryptanalysis, Black hole, Sybil, etc. Lightweight intrusion detection was proposed by Jan et al. using a supervised learning method.

2) IDS for Smart City

This work aims to protect smart cities against DDoS attacks by locating them within smart city apps. This study proposes a strategy that consists of two parts: a classifier model and an RBM model. Using this RBM model, high-level features can be learnt unsupervised. Using the classification, various distributed denial-of-service (DDoS) attacks can be differentiated.

3) IDS for Big Data Environment

The term "big data" refers to massive datasets that encompass a wide range of information types, including structured, unstructured, and semi-structured data. With such a large dataset, a traditional intrusion management system would fail. Machine learning methods are the exclusive way to implement intrusion detection systems in a big data environment.

4) IDS for Fog Computing

Fuzzy computing is an innovative approach to computer science that enhances speed by bringing analytics to the edge, where they can be utilized more efficiently. Cloud computing, fog computing, and the user layer comprise the three tiers that make up this architecture. Distributed fog nodes including routers, gateways, and edge servers form the fog service layer in fog computing.

5) IDS for Mobile

Communication and the storage of more sensitive information are two areas where mobile phones are rapidly gaining popularity. Potential security holes can be found in mobile apps, devices, networks, websites, and content [12]. Devices with IDS installed are better able to fend off these dangers. The 5G cyber defense architecture can detect cyberattacks in 5G mobile networks by utilizing a self-adaptive system based on deep learning. To classify the invasion, they plan to use a two-tiered architecture that includes the ASD and NAD modules.

III. Cloud Security Threat Landscape

Cloud computing has completely transformed the way computer services are provided, allowing users to access resources on demand and in a scalable manner. Due to its networked architecture, multi-tenancy, and dependence on virtualization, this paradigm change also introduces a large and dynamic danger landscape. Intrusion Detection Systems (IDS) and other effective countermeasures can only be developed after a thorough understanding of the types and extent of cloud-specific security threats has been gained. Here, we'll review the primary risks that cloud environments encounter in maintaining data privacy, integrity, and accessibility [13]. The reporting of past threats has been a valuable resource for understanding these shifts. Reports on security concerns across time provide a synopsis of relevant occurrences. An extensive collection of threat reports from the past is accessible; for example, a search for "cyber security threat report" on Google returns more than three million results. Either broad cybersecurity dangers or more targeted ones (such as web-based apps) might be included in these papers. While yearly and quarterly reports cover threats, all historical reports cover threats from the past. Cloud computing is the practice of using the Internet and other networked computers, storage devices, and software programs to host and supply computing resources to other users over the Internet [14]. Cloud services are accessible on demand and can be accessed using web browsers. There are numerous cloud computing solutions available, and each provider promises a specific level of service quality. The application, platform, and system layers are the three pillars upon which cloud computing rests.

E. Cloud Computing Architecture

Cloud computing refers to the fundamental design that enables the on-demand access to internet-based computer resources. It is a set of interconnected services and components that work together to provide efficient, scalable computing. Figure 2 shows that the architecture may be essentially broken down into two main parts: deployment models and service models.

1) Deployment Models

There are several models for deploying cloud services that consider factors such as ownership, access, and security requirements. [15]:

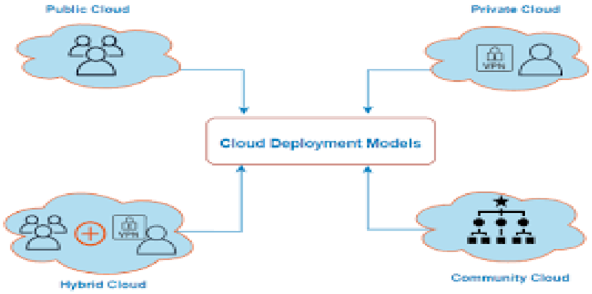

Fig. 2. Cloud Computing Deployment Model.

- **Private Cloud:** The organization or the cloud provider handles the maintenance of this private network infrastructure, which can be hosted on-premises or in the cloud. One reason it's more secure is that it restricts access to service delivery environments to the organization that controls it. It does not offer advantages such as lowering capital and operational expenses, but it does promise to address data security issues and provide greater control.
- **Public Cloud:** A cloud provider owns and operates this infrastructure, which is intended for use by various public groups. The resources are made available dynamically based on the pay-per-use model. Because it is vulnerable to hostile attacks, it is not very secure. Customers have several advantages, including scalability, independence from physical locations, flexibility, and the absence of the need to initially invest in infrastructure.
- **Hybrid Cloud:** This system enables users to access and share data and applications across multiple, geographically dispersed clouds using a network of interconnected, standardized computing resources. By combining their strengths and overcoming their weaknesses, they provide more application control and flexibility.
- **Community Cloud:** Multiple organisations within a single community with shared interests can utilise this cloud architecture. The community cloud makes all of its data and apps available to everyone at no cost. [16].

Artificial Intelligence (AI) has become a cornerstone in modernizing cloud security frameworks, enhancing the ability to detect and mitigate threats proactively. AI technologies such as machine learning (ML), deep learning (DL), and neural networks have proven to be powerful tools in securing cloud environments by identifying patterns, predicting threats, and responding to attacks in real time.

These technologies, particularly in cloud security, leverage large-scale data processing and analysis to continuously learn from new patterns, enabling systems to improve over time without human intervention.

Artificial Intelligence (AI) has become a cornerstone in modernizing cloud security frameworks, enhancing the ability to detect and mitigate threats proactively. AI technologies such as machine learning (ML), deep learning (DL), and neural networks have proven to be powerful tools in securing cloud environments by identifying patterns, predicting threats, and responding to attacks in real time.

These technologies, particularly in cloud security, leverage large-scale data processing and analysis to continuously learn from new patterns, enabling systems to improve over time without human intervention.

Artificial Intelligence (AI) has become a cornerstone in modernizing cloud security frameworks, enhancing the ability to detect and mitigate threats proactively. AI technologies such as machine learning (ML), deep learning (DL), and neural networks have proven to be powerful tools in securing cloud environments by identifying patterns, predicting threats, and responding to attacks in real time.

These technologies, particularly in cloud security, leverage large-scale data processing and analysis to continuously learn from new patterns, enabling systems to improve over time without human intervention.

Artificial Intelligence (AI) has become a cornerstone in modernizing cloud security frameworks, enhancing the ability to detect and mitigate threats proactively. AI technologies such as machine learning (ML), deep learning (DL), and neural networks have proven to be powerful tools in securing cloud environments by identifying patterns, predicting threats, and responding to attacks in real time.

These technologies, particularly in cloud security, leverage large-scale data processing and analysis to continuously learn from new patterns, enabling systems to improve over time without human intervention.

2) *Service Models*

Cloud services are offered under various models, depending on the level of control and abstraction provided to users.The service model architecture is shown in Figure 3:

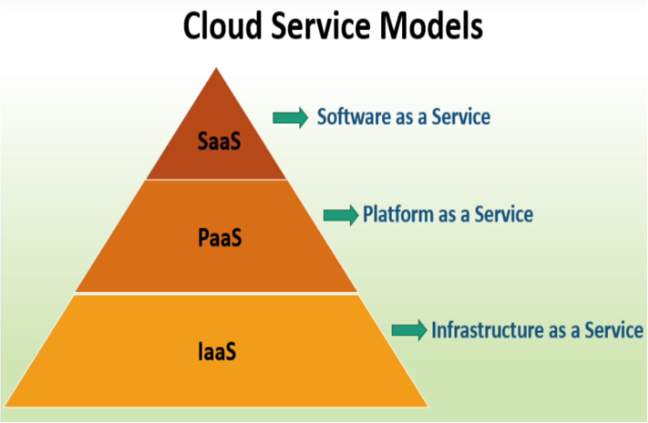

Fig. 3. Cloud Service Models.

a) *Software as a Service (SaaS)*

Consumers can access this typical kind of cloud service using any mobile application or web browser. Online apps that are completely operational are located on this top layer. Unlike the software bundles that users are required to purchase, the SaaS model provides software programs as internet-based services (see Figure 4). Thanks to cloud hosting, all processes and apps can be managed, eliminating the need for hardware installation or maintenance [17]. While most SaaS models are free, some may charge a subscription fee that can be paid monthly or annually to access additional features. Software-as-a-service (SaaS) models can be seen in several places, including Salesforce, Amazon Web Services, Google Cloud, Dropbox, and Google Workspace. Model for software services.

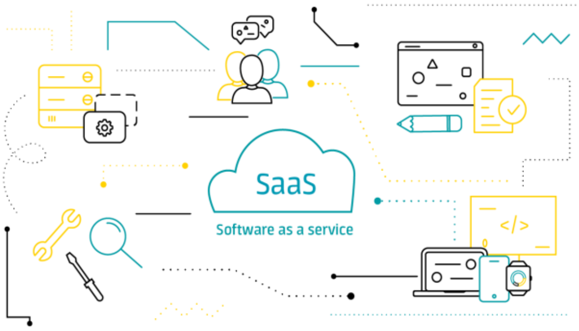

Fig. 4. Software as a Service (SaaS).

b) *Platform as a Service (PaaS)*

PaaS enables the complete application development lifecycle, from testing and design to implementation and debugging, by providing an operating system, hardware, and network infrastructure. The environment for development is web browsers. Apps can be built, tested, shared, maintained, and upgraded with the help of the PaaS paradigm, which creates a life-cycle model. Businesses can benefit from cloud developers' application software, web services, networks, and business strategies. The developer, who is also a user, can efficiently run the cloud system while reducing material expenses, thanks to the self-management nature of the platform as a service model. PaaS models are used in the cloud computing industry and include services such as Amazon Web Services (EC2), Google Cloud Platform, and Salesforce. System design for PaaS operations. The acronym "PaaS" is visible in Figure 5.

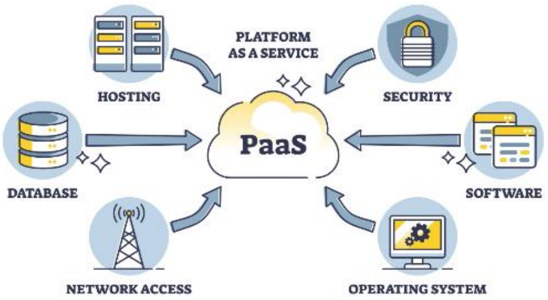

Fig. 5. Platform as a Service (PaaS).

c) *Infrastructure as a Service (IaaS)*

Virtual computers, storage, and networking are all part of the virtualized computer resources offered by Infrastructure as a Service, the lowest tier. Users can access the software, configurations, and operating systems of the virtualised resource. This cloud service provides its customers with the necessary networks, servers, data storage, and other computer resources to run their software and systems effectively (see Figure 6). As part of creating a cloud-based infrastructure as a service (IaaS), designers check that the model's operating system and virtualization are compatible with the machine's specifications. Among the several IaaS models, the most common ones include Cisco and IBM hardware services, as well as Amazon Web Services' S3.

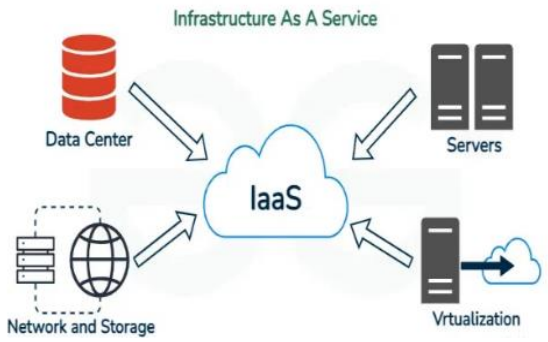

Fig. 6. Infrastructure as a Service (IaaS).

IV. Machine Learning And Deep Learning In IDS

Unsupervised learning relies on similarity-based clustering. Even with an unlabelled dataset, the model may discover the hidden pattern. Modelling techniques, such as grouping and association, allow it to unearth previously unseen patterns in the dataset. Artificial intelligence (AI) that learns from its own experiences, known as unsupervised learning, is a genuine phenomenon. In Figure 7, they can observe the integration of ML and DL into the IDS architecture.

Anomalies can also be identified using IDS techniques, which seek to detect any behaviour that deviates from the norm. The process is known by another name: misuse detection. The detection system relies solely on three components: training, detection, and parameterisation. The observed behaviours, such as hosts and network connections, are captured in the parameterization stage. Using the training module, a classification model may be built to determine if these behaviours are normal or aberrant.

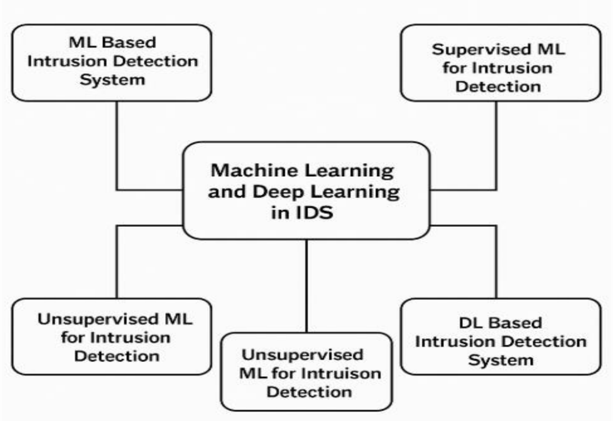
ML Based Intrusion Detection System
Supervised ML for Intrusion Detection
Machine Learning and Deep Learning in IDS
Unsupervised ML for Intrusion Detection
Unsupervised ML for Intruison Detection
DL Based Intrusion Detection System

Fig. 7. Machine Learning and Deep Learning in IDS.

F. ML-Based Intrusion Detection System

Security professionals rely on ML algorithms to foretell potential threats, thwart attacks, and prevent cybercrimes by erasing sensitive data. As a security measure, ML algorithms can predict potential attacks; this section primarily addresses the most popular ones. When developing an anomaly detection system that leverages ML the gold standard for attack detection it is crucial to have a firm grasp of the system's semantic characteristics. Understanding the threat model that is, the attacker's actions and the system's surroundings helps build an ML security solution [18].

1) Supervised ML for Intrusion Detection

The relationships between inputs and outputs provide the basis for an ML task's output data mapping. They have taken popular machine methods for intrusion detection into account for the empirical analysis. Using the training samples to accomplish a predetermined goal is the fundamental principle of supervised learning. Classification and regression procedures are typical examples of this type of learning.

2) Unsupervised ML for intrusion detection

Clustering based on similarities is the foundation of unsupervised learning. The model might still find the hidden pattern in an unlabelled dataset. Modelling techniques, such as grouping and association, allow it to unearth previously unseen patterns in the dataset. In reality, AI that learns from its own experiences, or unsupervised learning, is very similar to how people learn.

G. DL Based Intrusion Detection System

DL is a branch of ML That Has Developed quite a bit over the years. DL architectures employ layered structures to model intricate ideas. ANNs draw architectural cues from the human brain, which has a significant influence on DL architectures. In several areas, including image processing, speech recognition, and assault detection, the DL technique is currently being used. Regarding feature extraction, DL architectures differ from ML architectures. Data-driven designs will autonomously extract features, and the algorithm will self-correct based on its own mistakes.

V. Literature Review

These studies explore advanced intrusion detection, cybersecurity, and privacy solutions using deep learning, reinforcement learning, and cloud-edge architectures. They address challenges in EV charging, VANETs, smart surveillance, cloud security, and data privacy, achieving high accuracy and efficiency.

Basnet and Hasan Ali (2020) Note That Cybersecurity flaws inherent to the open communication layer pose a threat to the CIA of grid resources. To keep up with the increasing demand for electric vehicles, it is crucial to establish EVCS quickly and reliably. They propose new IDS that can detect DoS attacks in EVCS using deep learning. To detect and classify DoS attacks in the EVCS, the methods LSTMs and DNNs are utilised (in Python 3.7.8). The results show that both the DNN- and LSTM-based IDS achieved detection accuracy levels above 99% [19]. Hsu and Matsuoka (2020) present an anomaly network intrusion detection system based on DRL. In an instant, their system can adjust to various forms of network traffic. Three significant additions have been made to this publication. First, to demonstrate the generalisability of their strategy, they showcase their work on the popular NIDS benchmark datasets NSL-KDD and UNSW-NB15, in addition to a genuine university network log. The second part of the process was demonstrating the efficacy of their strategy through comparisons with three other prominent machine learning techniques and two affiliated published findings. Now, their model can process millions of packets per second on the network a feat it has accomplished three times [20].

Zeng et al. (2019) The rapid advancement of smart automobiles has sparked considerable interest in privacy and security concerns regarding VANETs. It is recommended to install a dependable, real-time intrusion detection system in the VCM, as it is where the OBU devices connect to the internet. Their end-to-end intrusion detection solution can automatically detect malware traffic for OBUs using DL. Since their proposed method does not utilize any attributes of sensitive data that humans have retrieved, but instead relies entirely on raw traffic, it stands apart from previous intrusion detection systems. The performance is compared with previous methods using both a public dataset and a dataset that simulates a real-life VANET. Through testing, they determined that their approach can improve performance while reducing resource use [21].

Kaskavalci and Gören (2019) note that the proliferation of smart surveillance is a direct result of the convenience and declining cost of related technology. Conventional security systems constantly record video footage to a storage device. The downside is that this shortens the lifespan of the hard drive and produces massive amounts of data. Footage captured by more modern devices with an Internet connection is saved to the cloud. Additional bandwidth needs and Cloud fees are associated with this capability. Utilizing the power of the cloud and the edge computing network, they offer a distributed and scalable surveillance architecture that leverages deep learning. Their design significantly reduces bandwidth and cloud costs by processing footage before transmitting it to the cloud [22].

Torkura et al. (2018) Users can access multiple CSSs in a unified and concurrent manner thanks to CSBs, which also mask the complexity of the cloud. As a result of integrating many components, security complexities arise, as well as API compatibility issues, among other security risks associated with this multi-cloud strategy. Other challenges include increased attack surfaces and hostile insider threats. Unveiling these security concerns necessitates innovative approaches. In response, this article introduces CS-BAuditor, a novel cloud security solution that monitors CSB resources in real-time for indicators of misuse or unauthorized modifications (such as incorrectly set bucket policies) and remediates them [23].

Sharma (2017) starts from point on the path to implementing the ad hoc cloud. When an ad hoc cloud customer stores their most sensitive data on the provider's infrastructure-less network, security becomes a significant concern. I've investigated these issues in my study. To advance the policy-making process for ad hoc cloud implementation, this study proposes a model of proactive security architecture that considers these aspects [24].

Stringent regulations regarding the protection of personal information currently impede Suzic and Reiter (2016). In this article, we highlight the ongoing work being conducted as part of the SUNFISH H2020 project to enable secure private cloud federations for public administrations. Data security regulations in diverse environments may be enforced across organisations, focusing on architectural components and operations. By combining the enforcement of security policies in real-time with post-execution verification of adherence, their solution enables proactive limitation of data flows in federated systems. By checking data flows for compliance with security regulations at the organisational and federation levels, this framework aims to facilitate secure service integration and data exchange in cross-entity settings [25].

Zhao et al. (2016) provide a DL-based architecture for disease-named entity identification. The first step is to combine the input feature embeddings at the word, character, and lexical levels. Then, by stacking many convolutional layers, the input is automatically processed. As a last step, we collect correlation information between close labels by applying the multiple label approach to the output layer, as mentioned earlier. Results from trials using the NCBI and CDR datasets show that ML-CNN can achieve top-tier results [26].

Table I is compiled from research on cybersecurity in the environments of EVCS, VANETs, smart surveillance, and clouds. These methods enhance intrusion detection, data security, and system performance in the face of challenges such as real-time processing and multi-cloud complexity, utilizing deep learning, reinforcement learning, and auditing systems.

Table 1: Summary of Key Studies on Intrusion Detection Systems for Proactive Cloud Security.

Authors	Study	Approaches	Key Findings	Challenges
Basnet & Hasan Ali (2020)	Finding EV Charging Stations Victimised by DoS Attacks	LSTM, DNN	The detection accuracy was greater than 99% for both models, with LSTM outperforming DNN in terms of F1, recall, and precision.	Protecting smart grids and EVCS from DoS threats
Hsu & Matsuoka (2020)	Anomaly-based IDS with self-updating capability	Deep Reinforcement Learning (DRL)	Outperforms classic ML methods; scalable to million-scale traffic in real-time	Self-updating under evolving traffic behaviors
Zeng et al. (2019)	Identifying intrusions in vehicular ad hoc networks	DL on raw traffic	High performance using raw traffic without manual feature extraction	Real-time accuracy with limited resources
Kaskavalci & Gören (2019)	Smart surveillance with edge-cloud computing	Distributed DL-based surveillance system	Reduces bandwidth usage and cloud storage costs	Real-time processing on edge devices
Torkura et al. (2018)	Secure cloud storage broker auditing	CS-BAuditor for continuous security monitoring	Detects misconfigurations and unauthorized changes in CSB	Multi-cloud integration and API interoperability
Sharma (2017)	Security in ad hoc cloud environments	Proactive security architecture model	Contributes to policy design in infrastructure-less ad hoc clouds	Data confidentiality in untrusted environments
Suzic & Reiter (2016)	Secure private cloud federation (SUNFISH project)	Real-time data flow restriction & post-execution conformance	Enforces security across federated public cloud infrastructures	Cross-entity data exchange in heterogeneous systems

VI. Conclusion and Future Work

Cloud computing has become increasingly significant in modern digital infrastructure due to the scalability and flexibility it provides to users and enterprises. Nevertheless, it is associated with high levels of security challenges, such as the increasing sophistication of cyberattacks on cloud environments. This survey has discussed the state of IDSs in the field of cloud computing paying increased attention to the emergence of intelligent systems based on ML and DL approaches following the traditional approaches to IDSs using rules. Combining cooperative IDS models, which involve one or more IDS agents working with different cloud providers, has shown promise in enhancing threat detection through the concept of knowledge sharing and filling in the gaps. Among the barriers overcome by these advancements, high false positive rates, privacy concerns with data, model interpretation, and the challenges associated with deploying resource-intensive DL models across large-scale, cloud-based environments in real-time, should be listed.

A perfect example of an AI-based IDS that can be deployed in real-time in resource-constrained clouds is one that is not only efficient and lightweight, but also one that clearly states why it believes what it claims to be true about its model. A more in-depth study is needed to explore the potential of giving IDSs the ability to learn and adapt to new online attack patterns through training and on-the-go improvements. Additionally, the federated learning and privacy-preserving approaches provide a good direction for allowing collaborative detection without compromising the confidentiality of user information. The creation of standardized benchmarks, realistic cloud-specific datasets, and evaluation metrics would also be key to the progress of research and deployment in this sensitive area of cloud protection.

References

1. A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *J. Netw. Comput. Appl.*, vol. 79, pp. 88–115, Feb. 2017, doi: 10.1016/j.jnca.2016.11.027.
2. A. Thakkar and R. Lohiya, "A Review of the Advancement in Intrusion Detection Datasets," *Procedia Comput. Sci.*, vol. 167, pp. 636–645, 2020, doi: https://doi.org/10.1016/j.procs.2020.03.330.
3. A. Abusitta, M. Bellaiche, M. Dagenais, and T. Halabi, "A deep learning approach for proactive multi-cloud cooperative intrusion detection system," *Futur. Gener. Comput. Syst.*, vol. 98, pp. 308–318, Sep. 2019, doi: 10.1016/j.future.2019.03.043.
4. S. Zhang, L. Yao, A. Sun, and Y. Tay, "Deep Learning Based Recommender System," *ACM Comput. Surv.*, vol. 52, no. 1, pp. 1–38, Jan. 2018, doi: 10.1145/3285029.
5. D. Rani and N. C. Kaushal, "Supervised Machine Learning Based Network Intrusion Detection System for Internet of Things," in *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*, 2020. doi: 10.1109/ICCCNT49239.2020.9225340.
6. S. Garg, "Predictive Analytics and Auto Remediation using Artificial Intelligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.
7. X. Li, J. Du, Y. Wang, and Y. Cao, "Automatic Sales Forecasting System Based On LSTM Network," in *2020 International Conference on Computer Science and Management Technology (ICCSMT)*, 2020, pp. 393–396. doi: 10.1109/ICCSMT51754.2020.00088.
8. N. Thapa, Z. Liu, D. B. Kc, B. Gokaraju, and K. Roy, "Comparison of machine learning and deep learning models for network intrusion detection systems," *Futur. Internet*, vol. 12, no. 10, pp. 1–16, 2020, doi: 10.3390/fi12100167.
9. T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," *Procedia Comput. Sci.*, vol. 171, pp. 1251–1260, 2020, doi: https://doi.org/10.1016/j.procs.2020.04.133.
10. S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Network.," *J. Crit. Rev.*, vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.
11. S. Garg, "AI/ML Driven Proactive Performance Monitoring, Resource Allocation and Effective Cost Management in SaaS Operations," *Int. J. Core Eng. Manag.*, vol. 6, no. 6, pp. 263–273, 2019.
12. M. Basnet; and M. H. Ali, "Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station," in *2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES)*, IEEE, Sep. 2020, pp. 408–413. doi: 10.1109/SPIES48661.2020.9243152.
13. Y.-F. Hsu and M. Matsuoka, "A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System," in *2020 IEEE 9th International Conference on Cloud Networking (CloudNet)*, 2020, pp. 1–6. doi: 10.1109/CloudNet51028.2020.9335796.
14. Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "DeepVCM: A Deep Learning Based Intrusion Detection Method in VANET," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 2019, pp. 288–293. doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00060.
15. H. C. Kaskavalci and S. Gören, "A Deep Learning Based Distributed Smart Surveillance Architecture using Edge and Cloud Computing," in *2019 International Conference on Deep Learning and Machine Learning in Emerging Applications (Deep-ML)*, 2019, pp. 1–6. doi: 10.1109/Deep-ML.2019.00009.
16. K. A. Torkura, M. I. H. Sukmana, T. Strauss, H. Graupner, F. Cheng, and C. Meinel, "CSBAuditor: Proactive security risk analysis for cloud storage broker systems," in *NCA 2018 - 2018 IEEE 17th International Symposium on Network Computing and Applications*, 2018. doi: 10.1109/NCA.2018.8548329.
17. Z. Zhao *et al.*, "ML-CNN: A novel deep learning based disease named entity recognition architecture," in *2016 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 2016, p. 794. doi: 10.1109/BIBM.2016.7822625.
18. Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., & Nandiraju, S. K. K. (2024). A Machine Learning-Based Framework for Predicting and Improving Student Outcomes Using Big Educational Data (Approved by ICITET 2024 Conference Proceedings). Available at SSRN 5315635.
19. Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., & Kakani, A. B. (2025). Towards Early Forecast of Diabetes Mellitus via Machine Learning Systems in Healthcare. European Journal of Technology, 9(1), 35-50.
20. Krutthika H. K. & Rajashekhara R. (2019). Network-on-chip: A survey on router design and algorithms. International Journal of Recent Technology and Engineering, 7(6), 1687–1691. https://doi.org/10.35940/ijrte.F2131.037619
21. Chalasani, R., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., & Tyagadurgam, M. S. V. (2025). Big Data-Driven Approach for Lung Cancer Identification via Advanced Deep Transfer Learning Models. European Journal of Technology, 9(1), 51-67.

22. Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., & Patchipulusu, H. H. S. (2024). Machine Learning-Based Approaches for Detecting and Mitigating Distributed Denial of Service (DDoS) Attacks to Improved Cloud Security. European Journal of Technology, 8(6), 28-48.
23. Krutthika H. K. & A.R. Aswatha. (2020). FPGA-based design and architecture of network-on-chip router for efficient data propagation. *IIOAB Journal*, *11*(S2), 7–25.
24. Polu, A. R., Narra, B., Buddula, D. V. K. R., Hara, H., Patchipulusu, S., Vattikonda, N., & Gupta, A. K. Analyzing the Role of Analytics in Insurance Risk Management: A Systematic Review of Process Improvement and Business Agility.
25. Madhura, R., Varshitha, P., Nikitha, S., Niveditha, K. M., & Bhat, M. (2024, December). RTL design of 16-bit RISC Processor Using Vedic Mathematics. In 2024 IEEE 33rd Asian Test Symposium (ATS) (pp. 1-4). IEEE.
26. Krutthika H. K. & A.R. Aswatha (2020). Design of efficient FSM-based 3D network-on-chip architecture. International Journal of Engineering Trends and Technology, 68(10), 67–73. https://doi.org/10.14445/22315381/IJETT-V68I10P212
27. Harinandan, R., Kumar, M., Vamshi, P., Padma, C. R., Krishnappa, K. H., & Raghunandan, J. R. (2024, August). Design and Development of a Real-time Monitoring System for ACL Injury Prevention. In 2024 2nd International Conference on Networking, Embedded and Wireless Systems (ICNEWS) (pp. 1-6). IEEE.
28. Krishnappa, K. H. (2024). Traffic pattern analysis for malicious node detection in NoC design. Journal of Communications, 9, 12.
29. Mukund Sai Vikram Tyagadurgam, Venkataswamy Naidu Gangineni, Sriram Pabbineedi, Mitra Penmetsa, Jayakeshav Reddy Bhumireddy, et al. (2024) AI-Powered Cybersecurity Risk Scoring for Financial Institutions Using Machine Learning Techniques. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-482. DOI: doi.org/10.47363/JAICC/2024(3)452.
30. HK, K. (2020). Design of Efficient FSM Based 3D Network on Chip Architecture. *INTERNATIONAL JOURNAL OF ENGINEERING*, *68*(10), 67-73.
31. Krutthika, H. K. (2019, October). Modeling of Data Delivery Modes of Next Generation SOC-NOC Router. In *2019 Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
32. Ajay, S., Satya Sai Krishna Mohan G, Rao, S. S., Shaunak, S. B., Krutthika, H. K., Ananda, Y. R., & Jose, J. (2018). Source Hotspot Management in a Mesh Network on Chip. In *VDAT* (pp. 619-630).
33. Nair, T. R., & Krutthika, H. K. (2010). An Architectural Approach for Decoding and Distributing Functions in FPUs in a Functional Processor System. *arXiv preprint arXiv:1001.3781*.
34. Gopalakrishnan Nair, T. R., & Krutthika, H. K (2010). An Architectural Approach for Decoding and Distributing Functions in FPUs in a Functional Processor System. *arXiv e-prints*, arXiv-1001.
35. Krutthika H. K. & A.R. Aswatha. (2021). Implementation and analysis of congestion prevention and fault tolerance in network on chip. *Journal of Tianjin University Science and Technology*, *54*(11), 213–231. https://doi.org/10.5281/zenodo.5746712.
36. Pabbineedi, S., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., Tyagadurgam, M. S. V., & Gangineni, V. N. (2023). Scalable Deep Learning Algorithms with Big Data for Predictive Maintenance in Industrial IoT. International Journal of AI, BigData, Computational and Management Studies, 4(1), 88-97.
37. Chalasani, R., Vangala, S. R., Polam, R. M., Kamarthapu, B., Penmetsa, M., & Bhumireddy, J. R. (2023). Detecting Network Intrusions Using Big Data-Driven Artificial Intelligence Techniques in Cybersecurity. International Journal of AI, BigData, Computational and Management Studies, 4(3), 50-60.
38. Vangala, S. R., Polam, R. M., Kamarthapu, B., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. (2023). A Review of Machine Learning Techniques for Financial Stress Testing: Emerging Trends, Tools, and Challenges. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(1), 40-50.
39. Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., Tyagadurgam, M. S. V., Gangineni, V. N., & Pabbineedi, S. (2023). A Survey on Regulatory Compliance and AI-Based Risk Management in Financial Services. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(4), 46-53.
40. Bhumireddy, J. R., Chalasani, R., Vangala, S. R., Kamarthapu, B., Polam, R. M., & Penmetsa, M. (2023). Predictive Machine Learning Models for Financial Fraud Detection Leveraging Big Data Analysis. International Journal of Emerging Trends in Computer Science and Information Technology, 4(1), 34-43.
41. Gangineni, V. N., Pabbineedi, S., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Tyagadurgam, M. S. V. (2023). AI-Enabled Big Data Analytics for Climate Change Prediction and Environmental Monitoring. International Journal of Emerging Trends in Computer Science and Information Technology, 4(3), 71-79.
42. Polam, R. M. (2023). Predictive Machine Learning Strategies and Clinical Diagnosis for Prognosis in Healthcare: Insights from MIMIC-III Dataset. Available at SSRN 5495028.
43. Narra, B., Gupta, A., Polu, A. R., Vattikonda, N., Buddula, D. V. K. R., & Patchipulusu, H. (2023). Predictive Analytics in E-Commerce: Effective Business Analysis through Machine Learning. Available at SSRN 5315532.
44. Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., Polu, A. R., Vattikonda, N., & Gupta, A. K. (2023). Advanced Edge Computing Frameworks for Optimizing Data Processing and Latency in IoT Networks. JOETSR-Journal of Emerging Trends in Scientific Research, 1(1).
45. Patchipulusu, H. H. S., Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., & Buddula, D. V. K. R. (2023). Opportunities and Limitations of Using Artificial Intelligence to Personalize E-Learning Platforms. International Journal of AI, BigData, Computational and Management Studies, 4(1), 128-136.
46. Madhura, R., Krishnappa, K. H., Shashidhar, R., Shwetha, G., Yashaswini, K. P., & Sandya, G. R. (2023, December). UVM Methodology for ARINC 429 Transceiver in Loop Back Mode. In 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-7). IEEE.

47. Shashidhar, R., Kadakol, P., Sreeniketh, D., Patil, P., Krishnappa, K. H., & Madhura, R. (2023, November). EEG data analysis for stress detection using k-nearest neighbor. In 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1-7). IEEE.
48. KRISHNAPPA, K. H., & Trivedi, S. K. (2023). Efficient and Accurate Estimation of Pharmacokinetic Maps from DCE-MRI using Extended Tofts Model in Frequency Domain.
49. Krishnappa, K. H., Shashidhar, R., Shashank, M. P., & Roopa, M. (2023, November). Detecting Parkinson's disease with prediction: A novel SVM approach. In 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE) (pp. 1-7). IEEE.
50. Shashidhar, R., Balivada, D., Shalini, D. N., Krishnappa, K. H., & Roopa, M. (2023, November). Music Emotion Recognition using Convolutional Neural Networks for Regional Languages. In 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE) (pp. 1-7). IEEE.
51. Madhura, R., Krishnappa, K. H., Manasa, R., & Yashaswini, K. P. (2023, August). Slack Time Analysis for APB Timer Using Genus Synthesis Tool. In International Conference on ICT for Sustainable Development (pp. 207-217). Singapore: Springer Nature Singapore.
52. Krishnappa, K. H., & Gowda, N. V. N. (2023, August). Dictionary-Based PLS Approach to Pharmacokinetic Mapping in DCE-MRI Using Tofts Model. In International Conference on ICT for Sustainable Development (pp. 219-226). Singapore: Springer Nature Singapore.
53. Krishnappa, K. H., & Gowda, N. V. N. (2023, August). Dictionary-Based PLS Approach to Pharmacokinetic Mapping in DCE-MRI Using Tofts Model. In International Conference on ICT for Sustainable Development (pp. 219-226). Singapore: Springer Nature Singapore.
54. Madhura, R., Krutthika Hirebasur Krishnappa. et al., (2023). Slack time analysis for APB timer using Genus synthesis tool. 8th Edition ICT4SD International ICT Summit & Awards, Vol.3, 207–217. https://doi.org/10.1007/978-981-99-4932-8_20
55. Shashidhar, R., Aditya, V., Srihari, S., Subhash, M. H., & Krishnappa, K. H. (2023). Empowering investors: Insights from sentiment analysis, FFT, and regression in Indian stock markets. 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), 01–06. https://doi.org/10.1109/AIKIIE60097.2023.10390502
56. Jayakeshav Reddy Bhumireddy, Rajiv Chalasani, Mukund Sai Vikram Tyagadurgam, Venkataswamy Naidu Gangineni, Sriram Pabbineedi, Mitra Penmetsa. Predictive models for early detection of chronic diseases in elderly populations: A machine learning perspective. Int J Comput Artif Intell 2023;4(1):71-79. DOI: 10.33545/27076571.2023.v4.i1a.169