Review

Intrusion Detection Systems for Cloud and IoT Infrastructures: Comprehensive Review of Challenges, Strategies, and Future Directions

Maryam Mahdi Alhusseini *

Posted Date: 24 March 2026

doi: 10.20944/preprints202603.1817.v1

Keywords: protection system; cloud computing; internet of things; intrusion detection system

 doi:10.20944/preprints202603.1817.v1

Review

Intrusion Detection Systems for Cloud and IoT Infrastructures: Comprehensive Review of Challenges, Strategies, and Future Directions

Maryam Mahdi Alhusseini

Information and Communication Technology Department, Polytechnic College of Engineering - Baghdad, Middle Technical University, Baghdad, Iraq; mariammahdi@mtu.edu.iq

Abstract

The rapid growth of Cloud Computing (CC) and Internet of Things (IoT) has brought numerous benefits to individuals and organizations, including cost savings, scalability, and flexibility. Nevertheless, the growing use of cloud services has become a source of security challenges too, especially the Intrusion Detection System (IDS). The functions of this review paper are to make sure that the IDS in CC and IoT is talked about in a way that is understood and has its meaning, concerns, and other approaches. The best contribution the paper has made is an extensive discussion of the types of IDS and their techniques, the analysis of the existing IDS solutions available in the cloud environments, and the discussion of the case studies related to the successful implementation of the IDS. Also, this paper sheds light on the future trends and research directions in the area, such as the use of Machine Learning (ML) and Artificial Intelligence (AI), the use of big data analytics, and the implications of cloud computing, IoT, and edge computing. This review can assist future researchers, practitioners, and policymakers and add to the establishment of, ultimately, more secure and resilient IoT and CC infrastructures by synthesizing existing knowledge and defining what gaps still exist in the literature.

Keywords: protection system; cloud computing; internet of things; intrusion detection system

1. Introduction

The Cloud is a term used to refer to a platform that utilizes shared servers and the Internet to deliver software, infrastructure, rules, and other functionality to customers, aiming to reduce their costs and complexity [1]. The availability of services on demand, Flexibility in resource allocation, high fault tolerance, and scalability are key factors contributing to CC's popularity. Cloud providers, including Google, Amazon, and Microsoft, use virtualization technology with self-service capabilities to do this [2].

The fast-developing Internet of Things (IoT) has increased network connections dramatically, creating complicated cybersecurity issues. In this dynamic environment that is prone to ever-changing and advanced cyber threats, traditional intrusion detection systems (IDS) cannot effectively detect them. In order to overcome these weaknesses, the intelligent use of AI and Deep Learning (DL) has been implemented to detect anomalies intelligently. Nevertheless, the optimization of deep learning models is still significant for high accuracy and fewer false alarms. In this work, a hybrid intrusion detection system (HyIDS) that combines Energy Valley Optimizer (EVO) and Snake Optimizer (SOA) algorithms is proposed to improve the performance of deep learning in IoT network security [3].

The volume of data generated daily has increased dramatically, driven by the growing demand for IT services [4]. However, attackers who profit from the vast amounts of data produced by CC, which can reach up to 665 Gb/s [5], have also taken notice of this. Massive data production has emerged as one of CC's primary challenges, as it makes it an attractive target for online criminals [6].

 doi:10.20944/preprints202603.1817.v1

Hackers are particularly drawn to the cloud due to its open and distributed structure and the large amount of traffic it generates [7].

By interfering with user services, abusing sensitive data, and exploiting the CSP's resources, cybercriminals put CC services at risk. These invasions may entail the misuse of sensitive information or the irrational use of CPU, bandwidth, and storage. Firewalls and other traditional security measures often fall short of providing the level of protection required for telecommunications services. To protect consumers from cyber threats, a more effective security system is needed.

By examining network data, an IDS may be used to identify network threats. Based on deployment methodologies, IDS may be divided into two primary groups: host-based IDS and network-based IDS [8,9]. A network-based IDS scans the entire network for evidence of an intrusion, whereas a host-based IDS monitors the host system and identifies attacks by analyzing data from each node. Each cloud node that uses a host-based IDS has a separate IDS and storage system.

IDS may also be divided into two categories based on the method of detection: these categories are signature-based IDS and anomaly-based IDS. By comparing network traffic with the attack signatures stored in the database, a signature-based IDS can identify attacks. Anomaly-based IDS, in contrast, builds a profile of network behavior by examining dynamic user, application, and user activity over a predetermined time period to identify any suspicious or unusual behavior [10,11].

Due to the shared, dynamic, and dispersed nature of cloud systems, intrusion detection plays a significant role in CC [12]. Organizations are more susceptible to cyber threats, such as malware attacks, unauthorized access, and data breaches, when they migrate their data and applications to the cloud [13]. The confidentiality, integrity, and accessibility of data in the cloud can be ensured by an efficient IDS, which can help identify and prevent these threats. Implementing robust intrusion detection techniques is crucial for maintaining client confidence and fulfilling compliance obligations, as cloud service providers must adhere to numerous industry-specific laws and standards.

The peculiarities of CC and IoT present several challenges when developing and implementing IDS [14]. The sheer volume of network traffic, the dynamic and multi-tenant nature of cloud resources, the need for real-time threat detection and response, and the protection of user privacy are among these challenges. This review paper's primary goal is to provide readers with a comprehensive overview of the current status of IDS in CC, while highlighting various strategies, techniques, and best practices for addressing these challenges. The report also aims to highlight the shortcomings of current solutions and explore potential future research avenues in this area.

This review article discusses various aspects of IDS in CC and IoT. The scope encompasses a comprehensive analysis of various IDS types and approaches, a comparison of current solutions in cloud environments, and an examination of CC concepts and security concerns. The report also examines real-world case studies, lessons learned, and potential directions for IDS study and future growth. The essay is divided into several sections, beginning with an introduction and historical context, followed by a discussion of CC and IoT of IDS ideas. The conclusion highlights the major conclusions and contributions. The subsequent sections focus on the implementation of IDS in CC and IoT, case studies, and future research objectives. The Contributions of this paper:

1. Offering a critical overview of the IDS in Cloud Computing (CC) and IoT
2. Comparing the existing solutions and pointing out their strengths/weaknesses
3. The evaluation of the case studies and the lessons learned
4. Proposing directions for future research to develop IDS

2. Literature Review

2.1. Overview and Key Concepts of Cloud Computing

CC is a new development in information technology (IT) that moves processing and data away from traditional desktop and laptop computers to massive data centers [15]. Through the Internet, this technology enables users to access computing resources and software as needed, whenever they want, from any location. Without needing end users to be aware of the precise location or system

 doi:10.20944/preprints202603.1817.v1

configuration of the system delivering the services, CC primarily deals with the supply of compute, data storage, and software services [16].

The National Institute of Standards and Technology (NIST) defines CC as a model that enables convenient and on-demand network access to a shared pool of reconfigurable computing resources, including data storage, servers, networks, software applications, and other computing services that can be quickly provisioned and released with little management effort or interaction with the service provider [17]. CC drastically lowers the cost of computer services by pooling resources.

2.2. Cloud Architecture

In a CC system, the front end and back end are two separate components [18]. A CC system's front end and back end are linked via a network, often the Internet. The user or client interacts with the front end, which includes their computer and the browser program they use to access the cloud. The CC services, such as on-demand computation and data storage, provided by numerous servers, comprise the back end (as illustrated in Figures 1 and 2). The following diagram illustrates the differences between a standard computer system and a CC system. Hardware virtualization is a method used in CC that allows many operating systems, or guests, to operate concurrently on a host machine. This is achieved by using a hypervisor, sometimes referred to as a virtual machine manager (VMM), which operates at a level above supervisory software. The VMM, often referred to as a hypervisor, provides a virtual operating platform for the guest operating systems and controls how they are run. Different operating system instances can share the virtualized hardware resources. Hypervisors are typically installed on server hardware to run guest operating systems that can act as servers.

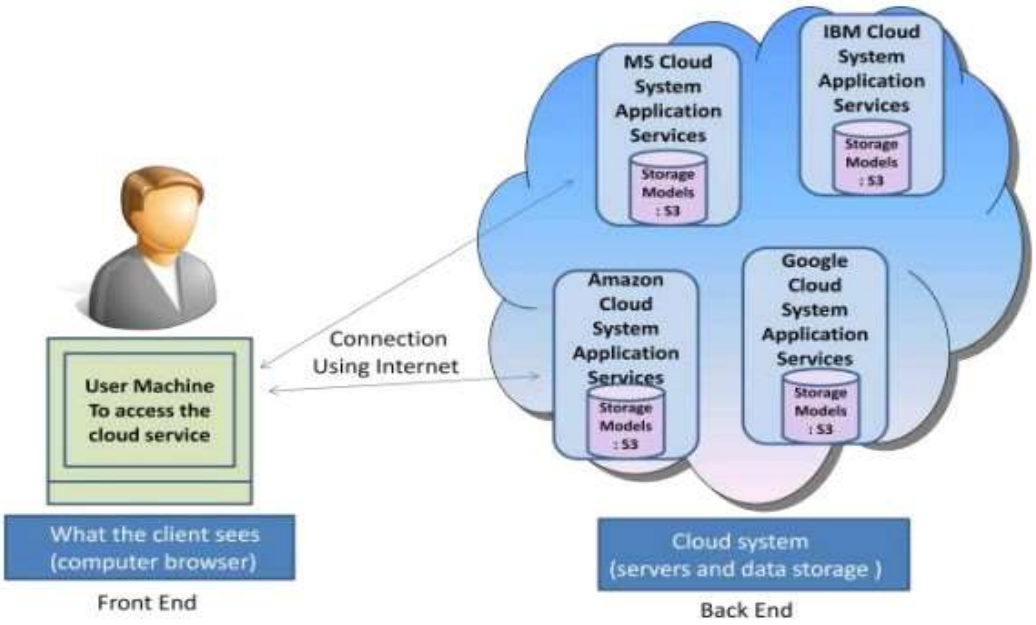

Figure 1. Cloud Architecture [18].

2.3. Cloud Computing Characteristics

A contemporary technology called CC offers elastic, on-demand, virtualized, cost-effective computer resources [19]. CC significantly reduces costs and prevents resource and processing power wastage by leveraging the infrastructure provided by a third party. Combining distributed resources to increase throughput and effectively tackle complex computation problems is the primary goal of CC. On-demand self-service, where computer resources are delivered online according to the client's needs without human intervention, is one of the most significant aspects of CC. Without relying on client systems, cloud users may access a wide variety of cloud services through the Internet [20].

 doi:10.20944/preprints202603.1817.v1

According to demand, resources are pooled to service a variety of customers, and utilization may be tracked and managed for transparency. For quality service, choosing a reputable and trustworthy cloud service provider is essential. Users should select service providers with good customer service and a track record of success in IT-related activities.

Table 1. Key Characteristics of Cloud Computing.

Key Characteristics	Description
self-service and computing resources	On-demand Online self-service and computing resources are made available at predetermined times without involving any human engagement on behalf of the customer. Regardless of other software and hardware, users of CC can access data, apps, or any other services only through a browser.
Broad Network Access	Cloud customers have access to a wide range of cloud services that are available online. The client platform is not required to access cloud services. Services are available 24/7, wherever and at any time.
Resource Pooling	In response to consumer demand, a pool of CC resources is used to support many customers.
Measured Service	Since cloud systems automatically manage all computing resources, cloud users do not need to manage or optimize them. To ensure transparency for both the service provider and the user of the consumed resource, resource utilization can be tracked, managed, and reported.
Selection of Provider	To receive decent service, choosing a cloud service provider is essential. Users may choose the best service provider based on their preferences and understanding of cloud providers. One must confirm that the supplier is trustworthy, has a solid reputation for providing excellent customer care, and has a successful history working on IT-related projects.

2.4. Cloud Delivery Model

Three delivery types are available with CC: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [21]. Cloud deployment options for these models include public, private, community, and hybrid clouds. We can observe the management rights of the cloud user and the cloud provider over various tiers of the cloud system in the following diagram [22]. Refer to Figure 2.

Users of the cloud delivery model known as SaaS do not need to handle the setup and configuration of any hardware or software [23]. The vendor or cloud provider oversees all services. Google Online Office, Google Docs, and Email Cloud are a few examples of SaaS [24]. Reduced upfront costs, the possibility for lower lifetime costs, the elimination of license risk, and the elimination of

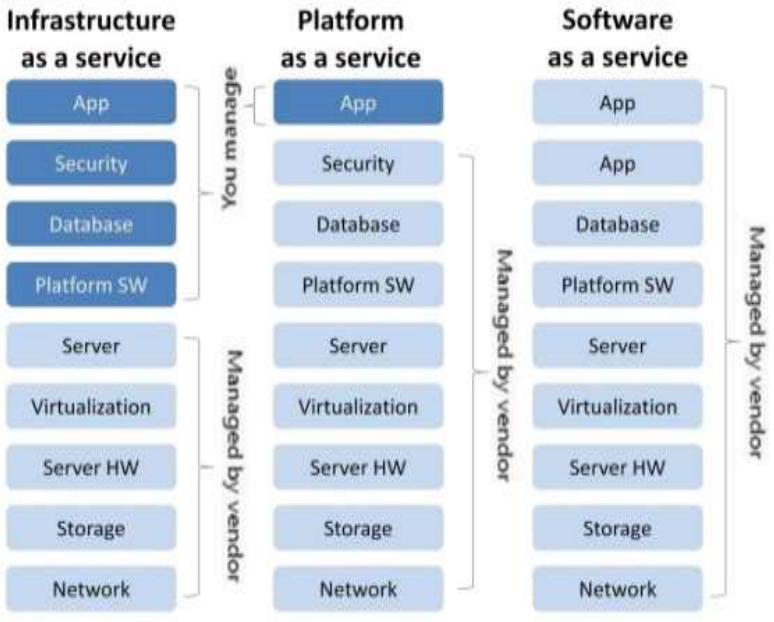

Figure 2. Cloud Delivery Mode [22].

 doi:10.20944/preprints202603.1817.v1

Version compatibility and a smaller hardware footprint are two key benefits of SaaS. The primary drawbacks are the synchronization of client and vendor migrations, as well as the administration of billing.

PaaS refers to the provision of a computing platform over the Internet, enabling customers to build and deploy their own programs as needed. The vendor or cloud provider is responsible for managing the configuration of the server and computing platform. Without the hassle of purchasing and operating storage servers, databases, and other software/hardware, web applications may be established rapidly. Google App Engine is one example of a PaaS [25]. PaaS eliminates hardware dependencies, offers an immediate global platform, frees developers to concentrate on application code, and has built-in scalability. The drawback is that stringent governance is necessary to prevent lines of business from developing apps without consulting IT. IaaS is a cloud provider's on-demand service that offers infrastructure, including servers, software, and networking hardware [26]. It scales up and down quickly to meet demand and can be utilized to eliminate the need for purchasing, housing, and managing the fundamental hardware and software infrastructure components. Amazon EC2 is an illustration of IaaS.

Table 2. Summary of Cloud Delivery Models.

Delivery Model	Description	Examples
SaaS	Managed software delivery	Google Online Office, Google Docs, Email cloud
PaaS	Managed platform delivery	Google App Engine
IaaS	Managed infrastructure delivery	Amazon EC2

3. Overview of Internet of Things (IoT Environments)

The Internet of Things (IoT) is a complex system of interrelated and connected devices and systems, encompassing both simple home appliances (e.g., thermostats and TVs) and more sophisticated systems, such as traffic lights and industrial equipment [27]. The proliferation of Internet of Things (IoT) devices and the increasing adoption of edge computing have significant implications for IDS in cloud environments [28]. With billions of IoT devices connected worldwide, these devices generate vast amounts of data that need to be processed, analyzed, and secured. Often, IoT devices have limited processing power and security capabilities, making them attractive targets for cybercriminals. Refer to Figure 3.

4. Research Questions and Hypotheses

Table 4. Research Questions and Hypotheses.

List	Research Questions	List	Hypothese
RQ1	How do current IDS architectures (host-based, network-based, hybrid) scale to the distributed, multi-tenant cloud computing environments?	**H1**	The hybrid IDS architecture will be more scalable and have less detection latency than host-based and network-based IDS in the distributed multi-tenant clouds.
RQ2	How far can signature-based, anomaly-based, and specification-based techniques fulfill the detection requirements of cloud/IoT settings about false positive and false negative rates?	**H2**	The IDS methods based on anomaly detection will detect novel attacks more effectively, but will generate more false positives compared to signature-based models. The hybrid methods can achieve a balance between the two measures.
RQ3	What are the efficacies of Deep Learning-based IDS models (e.g., RNN, GRU, LSTM, CNN), when compared to classical Machine Learning approaches (e.g., RF, SVM, KNN) in identifying zero-day and low-frequency attacks?	**H3**	The IDS built using deep learning (in particular, GRU/LSTM) will be more effective at evading zero-day and low-frequency attacks than the classical ML methods, with greater recall and F1-score.
RQ4	How can IDS be designed to protect data privacy and ensure compliance with regulations, while also facilitating deep packet inspection and traffic analysis?	**H4**	Models of privacy-preserving IDS (e.g., federated learning, homomorphic encryption) will maintain the same accuracy while minimizing the chances of data leakage in cloud and IoT networks.

 doi:10.20944/preprints202603.1817.v1

5. Intrusion Detection Systems (IDS)

Computer security is a field that focuses on identifying hostile activity in computer systems, such as invasions, penetrations, and other types of computer misuse. Utilizing IDS, which examines network or system operations to find vulnerabilities and exploits in a computer system [30], is one of the most important aspects of computer security. IDS can be categorized into host-based, network-based, and wireless IDS, and a hybrid IDS can be created by combining these subcategories. System files, system logs, and registry keys must be secure, and HIDS is responsible for monitoring the operation of each host. Since intrusion activities differ from routine system activity, anomaly detection techniques are frequently used in IDS.

A security technology called an IDS is used to track and examine network or system activity to look for potential policy violations or malicious activity [31]. An IDS's primary objective is to identify suspicious activity and notify system administrators or security staff so they can take the necessary precautions to mitigate the risks [32]. IDS is a crucial component in keeping computer systems and networks secure, as it adds a layer of defense against online attacks to existing security tools, such as firewalls and antivirus software [33].

Categories of IDS

Based on the data gathering techniques [34], IDS may be divided into two primary categories: host-based and network-based. To safeguard a system from network-based attacks, a network-based IDS (NIDS) is created to track and analyze data from network traffic. In contrast, host-based IDS (HIDS) tracks and examines information from system log files that are active on a specific system.

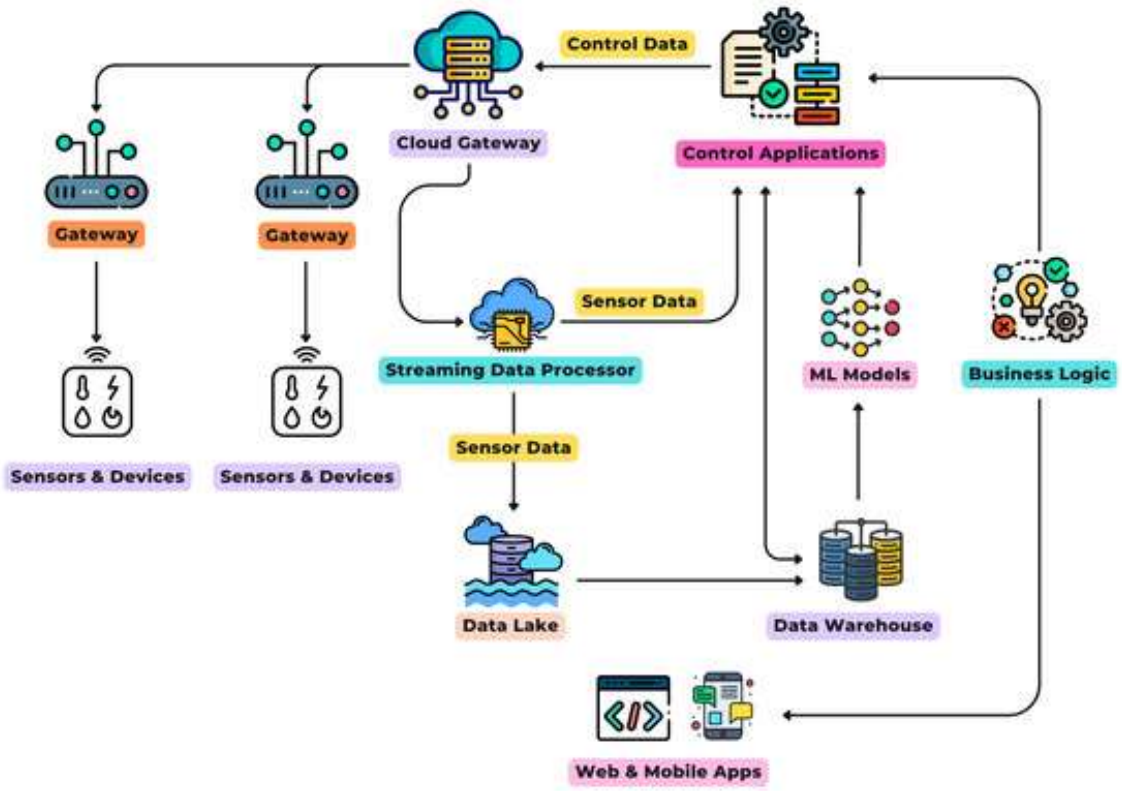

Figure 3. IoT Architectures [29].

IDS can be categorized according to intrusion detection methodologies and data collection methods [35]. Misuse-detection, specification-based detection, and anomaly-based detection are the three types of intrusion detection approaches [36]. Attacks are detected by misuse detection, which involves comparing them to known attack signatures. In specification-based detection, a set of

 doi:10.20944/preprints202603.1817.v1

guidelines for appropriate conduct is established, and any departures from these guidelines are marked as potential intrusions. On the other hand, anomaly-based detection involves identifying intrusions by detecting patterns that deviate from typical system activity. IDS employs various techniques to identify potential intrusions:

1. Signature-based IDS [37]: This Technique relies on a database of known attack patterns, also known as signatures. Signature-based IDS compares network or system activities with these signatures to identify potential threats. While effective against known attacks, this Technique may not detect new or previously unknown attacks.
2. Anomaly-based IDS [38]: Anomaly-based IDS monitors network or system activities and establishes a baseline of normal behavior. It then detects potential intrusions by identifying deviations from this baseline. This Technique can detect new and unknown attacks, but may produce false alarms due to legitimate variations in behavior.
3. Specification-based IDS [39]: Specification-based IDS uses predefined rules or policies that describe the correct operation of a system or application. The IDS detects intrusions by identifying activities that violate these rules or policies. This Technique can detect both known and unknown attacks, but requires a deep understanding of the monitored systems and their correct operation.
4. For the Evaluation of IDS, the performance of an IDS involves several metrics [40]:
5. Accuracy (ACC): The accuracy of an IDS refers to its ability to classify events as either usual or malicious correctly. A higher Acc indicates a better-performing IDS.
6. Detection rate: Also known as the actual positive rate, the detection rate measures the percentage of actual intrusions that the IDS correctly identifies. A high detection rate is desirable, as it indicates the IDS's effectiveness in identifying threats.
7. False alarm rate: The false alarm rate, also known as the false positive rate, measures the proportion of legitimate occurrences that the IDS incorrectly labels as malicious. A low false alarm rate is essential, as a high rate may lead to unnecessary resource consumption and reduced trust in the IDS's alerts.

6. IDS in Cloud Computing (CC)

IDS is a significant influence on cloud security. Cloud viruses, worms, password cracking, DDoS attacks, scanning, and the insertion of malware codes are increasing. Unless the attacks are detected early enough, they will harm the company's reputation and revenues. Numerous researchers have suggested detection techniques for cloud attacks [41]. There are four types of CC based IDS. These types are shown in Figure 4.

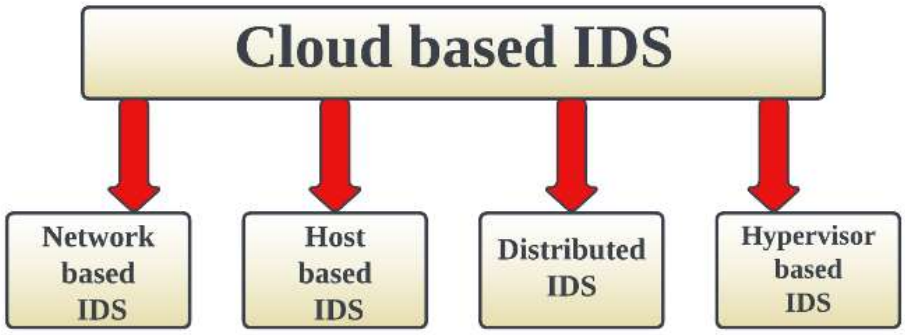

Figure 4. Types of Cloud-based IDS [Adapted from 42].

Challenges and Requirements of CC

Implementing IDS in CC environments presents a unique set of challenges and requirements. Some of the main concerns include [43]:

 doi:10.20944/preprints202603.1817.v1

1. Scalability: Highly scalable CC environments enable the provisioning and release of resources as needed. IDS installed in these contexts must be able to handle this dynamic nature, dynamically adjusting to changes in resource allocation and network traffic without compromising performance or efficacy.
2. Multi-tenancy: Multiple tenants who each of which has its own data, applications, and users, frequently share cloud services. IDS must be able to differentiate between the actions of various tenants, safeguarding the security and privacy of each tenant's data while also being capable of quickly identifying intrusions.
3. Elasticity: The elasticity of CC enables the dynamic addition and removal of resources, which can lead to changes in network traffic and system behavior. IDS must handle these oscillations, and its detection techniques must be adjusted correspondingly.
4. Virtualization: Virtualization technology, on which CC is primarily dependent, can make the implementation of IDS more difficult. IDS must be able to track and examine traffic in virtualized settings, taking into consideration the unique characteristics and challenges of virtual networks and systems.
5. Distributed architecture: Distributed architectures, in which resources are dispersed over several physical locations, are frequently used in CC. IDS may find it more challenging to gain a complete picture of network activity due to this dispersion, necessitating the deployment of multiple IDS instances and the effective aggregation of data from these instances.
6. Real-time detection and response: Rapid security incident detection and response are essential in CC environments to reduce the potential impact of an intrusion. To reduce damage and control the danger, IDS must be able to recognize threats in real-time and, where practical, automate the reaction.
7. Data privacy and compliance: IDS must safeguard user privacy and support compliance requirements, as cloud service providers are required to adhere to various data privacy laws and industry-specific standards. This entails ensuring that, when monitoring and analyzing network traffic, the IDS does not unintentionally disclose sensitive information or violate privacy laws.

To address these challenges and requirements, IDS solutions for CC should incorporate features such as auto-scaling, tenant-aware monitoring, adaptive detection mechanisms, virtualization-aware analysis, distributed data aggregation, real-time detection and response capabilities, and strict adherence to data privacy and compliance standards.

7. IDS in Internet of Things (IoT)

The Internet of Things (IoT) can be considered a universal network system comprising a multitude of networked devices that are based on sensing, communication, networking, and information processing technologies [44]. The Internet of Things (IoT) is a worldview that empowers the interconnection and communication of various physical and virtual devices via the Internet. IoT Networks find applications in various sectors, including smart cities, healthcare, agriculture, and transportation. Whatever the case, IoT networks also face numerous security threats, including unauthorized access, data theft, denial-of-service attacks, and malicious attacks. With this, the execution and planning of powerful intrusion detection systems (IDS) for IoT establishments is essential to protect their systems against probable threats and ensure their uninterrupted quality and availability. The Internet of Things (IoT), which encompasses machines, sensors, and cameras, continues to increase the number of devices connected to the Internet [45].

7.1. Challenges and Requirements of IoT

As IoT devices are rapidly being adopted in areas such as smart homes, healthcare, and industrial control systems. Strong intrusion detection systems (IDS) are urgently required that are capable of properly identifying diverse cyber-attacks while minimizing the number of false positives.

 doi:10.20944/preprints202603.1817.v1

A variety of IoT applications, along with their respective data types and attack vectors, necessitate the flexibility of IDS frameworks to offer comprehensive protection against the numerous types of threats [46]. With the ever-evolving nature of IoT security, the development of IDS techniques is an important field of research. The adoption of machine learning (ML) and deep learning (DL) approaches, along with improved feature selection and data preprocessing procedures, can lead to more effective IDS solutions [46].

To address these challenges, future research and development efforts should focus on designing and implementing IDS solutions that can effectively monitor and secure IoT devices and edge computing infrastructures. This may involve the development of lightweight, resource-efficient IDS algorithms that can be deployed on IoT devices or edge nodes, as well as the use of machine learning and AI techniques to analyze and correlate data from disparate sources to identify potential intrusions. Furthermore, the seamless integration of IoT, edge, and cloud-based IDS components will be critical in ensuring the comprehensive protection of these complex and interconnected environments. Refer to Figure 5

Figure 5. Key Challenges in IoT Environments [47].

7.2. Existing Approaches and Methodologies

Various strategies have addressed the difficulties of deploying IDS in CC systems and approaches [48]. Deploying virtualized IDS instances, which are easily scalable and adaptable to the dynamic nature of cloud resources, is one such strategy. The detection capabilities of IDS are also being enhanced by the use of machine learning and artificial intelligence techniques to better identify new and previously unidentified threats [49]. Researchers have also suggested using software-defined networking (SDN) to facilitate easier monitoring and analysis of network traffic in cloud settings [50], thereby providing greater granular control and visibility over network activity. Table 3 provides a comprehensive summary of related works in the field of intrusion detection.

Table 3. Summary of related works.

Ref.	Performance Evaluation	Dataset	Techniques	Out comes
[51]	Acc, precision (Prec), Recall (Rec), F1-s	RedIRIS	RNN and CNN	Modified hidden layers improved the algorithms
[52]	Acc, Prec, Rec, F1, FAR	KDD 99 Cup	GRU and RF	Loss function minimization improved results

 doi:10.20944/preprints202603.1817.v1

[53]	Acc, Prec, Rec, F1 measure	NSL-KDD	DNN	Used SGD to minimize the DNN's loss function
[54]	Acc, Prec, Rec	CICIDS2017	MLP, 1d- CNN, LSTM, CNN+LSTM	Balanced dataset through data processing
[55]	Prec, Rec (TPR), F1 s	NSL-KDD	DBN	Optimized DNN with cost function per layer
[56]	Acc, Prec, Rec, F1 m	NSL-KDD	SDPN	SMO algorithm optimized feature selection
[57]	Acc, Prec, Rec, F1 m	NSL-KDD	RF	Used the Weka tool for evaluation
[58]	Acc, Prec, Rec, F1 m	NSL-KDD, KDD99	ANN	Proposed stack-based feature selection
[59]	F1 s	Bot-IoT	RF, NB, and MLP	Utilized a hierarchical approach for intrusion detection
[60]	Acc, Prec, Rec, F1 m	CICIDS2017	HW-DBN	Detected a frequency attack

Systems, focusing on performance evaluation metrics, datasets, algorithms, techniques, and key findings. The studies were conducted between 2017 and 2025, employing various deep learning techniques and approaches to enhance the detection capabilities of these systems.

In 2023, work [61] The use of an EVO-based feature selection method reduced the number of features (80) to 43 on the CSE-CIC-IDS2018 dataset, which boosted the accuracy, precision, and recall of the SVM, RF, Decision Tree, and KNN models, thus increasing the efficiency of the IDS at lowering the cost of computation.

In recent years, a 2024 study [62] has explored the topic of secure data hiding methods, which involve integrating encryption and multimedia steganography to enhance communication security. For example, a new method utilizes Laplacian of Gaussian (LoG) edge detection in conjunction with ChaCha20 encryption to embed ciphertext into video frames with minimal visual corruption, thereby achieving high resistance to cyberattacks. These can be utilized in IDS to ensure that alerts are conveyed safely, that logs are stored in a manner that cannot be tampered with, and to secure sensitive information when intelligence is being gathered on the network.

In 2025, work [63] presents a better CAST-128 encryption based on chaos-based adaptive S-box generation (utilizing the Logistic Sine Map), which is more non-linear and avalanche-based, and resistant to statistical attacks. Therefore, it can be adopted in data stream security for communications and IDS data.

Table 3 highlights the progression of research in intrusion detection systems, demonstrating how various methods, techniques, and algorithms have been employed and adapted over the years to address emerging challenges and improve system performance.

8. Integrating IDS with Other Security Components (Advances in Machine Learning and AI for IDS)

Integrating IDS with other security measures, such as firewalls and encryption techniques, is crucial to maximizing their efficacy in CC settings [64]. Current research starting in 2024 has shown an even stronger focus on the role of feature selection in enhancing the performance of IDS, and especially finding methods to decrease computational cost and minimize false positive rates without degrading detection performance. As an example, Alzubi et al. [65] compare a self-selection of a range of metaheuristic FS algorithms (Grey Wolf, Bat, Pigeon-inspired) and demonstrate that it is possible to maintain the performance of IDS at rates close to 99% accuracy, even when scaling down gigantic feature spaces to minute subsets. Alhusseini et. al. [62] proposed Hybrid AI-Driven Intrusion Detection: Framework Leveraging Novel Feature Selection to Improve Network Security uses the Energy-Valley Optimization (EVO) technique on NSL-KDD to improve the coverage of features to 18

 doi:10.20944/preprints202603.1817.v1

features instead of 42 with minimal loss of accuracy. IDS and firewall integration can enhance the overall security posture by providing supplementary defense against various types of attacks. In Empirical Enhancement of Intrusion Detection Systems: A Comprehensive Approach with Genetic Algorithms-based Hyperparameter Optimization and Hybrid Feature Selection, as well, [66,67] combine the two and demonstrate the increase in F1-score and the decrease in false alarms. Alsaffar et al. [68] introduced improving intrusion detection with hybrid feature selection and stack ensemble learning involves a hybrid (filter + wrapper) feature selection algorithm (MI-Boruta) with a stacked ensemble, and demonstrates significant improvements in recall and precision with multiclass attacks. For instance, IDS can identify harmful activity that may have evaded firewall protections, whereas firewalls can stop unauthorized access to network resources. The security of cloud environments can be further enhanced by utilizing encryption technologies to protect sensitive data from interception or alteration during transmission or storage. Organizations can create a more comprehensive and resilient defense against cyberattacks by integrating these security components, thereby protecting the confidentiality, integrity, and availability of their data and cloud-based applications [69].

9. Future Trends and Research Directions

One of the Internet of Things future trends in the IDS research area is the incorporation of AI and ML to enhance the detection of new and sophisticated threats that the traditional approaches could not detect. ML and deep learning allow IDS to become more adaptive to recent changes in attack patterns by learning based on past data, and NLP and knowledge representation can make it more context-aware, minimize false alarms, and handle data that can be read by humans. Despite the positive outcomes of the approaches, there are still problems in terms of data quality, model transparency, and explainability. Future studies must focus on resolving these challenges to maximally use AI/ML to enhance and more capable IDS in the world of cloud computing [35,46–50,54,60].

10. Conclusions

10.1. Summary of Key Findings

The present review paper is a complete overview of the IDS in the environment of CC and IoT, in which the significance of intrusion detection is discussed, the types of IDS, as well as the methods to meet them. The special challenges and requirements of the implementation of IDS in the cloud have also been discussed and current methods, methods and solutions to tackle issues have been discussed. Moreover, we have addressed the aspects of integrating IDS with other security components and outlined the latest trends and research directions in the field, including the use of machine learning and AI techniques and the impact of IoT and edge computing on cloud-based IDS.

 doi:10.20944/preprints202603.1817.v1

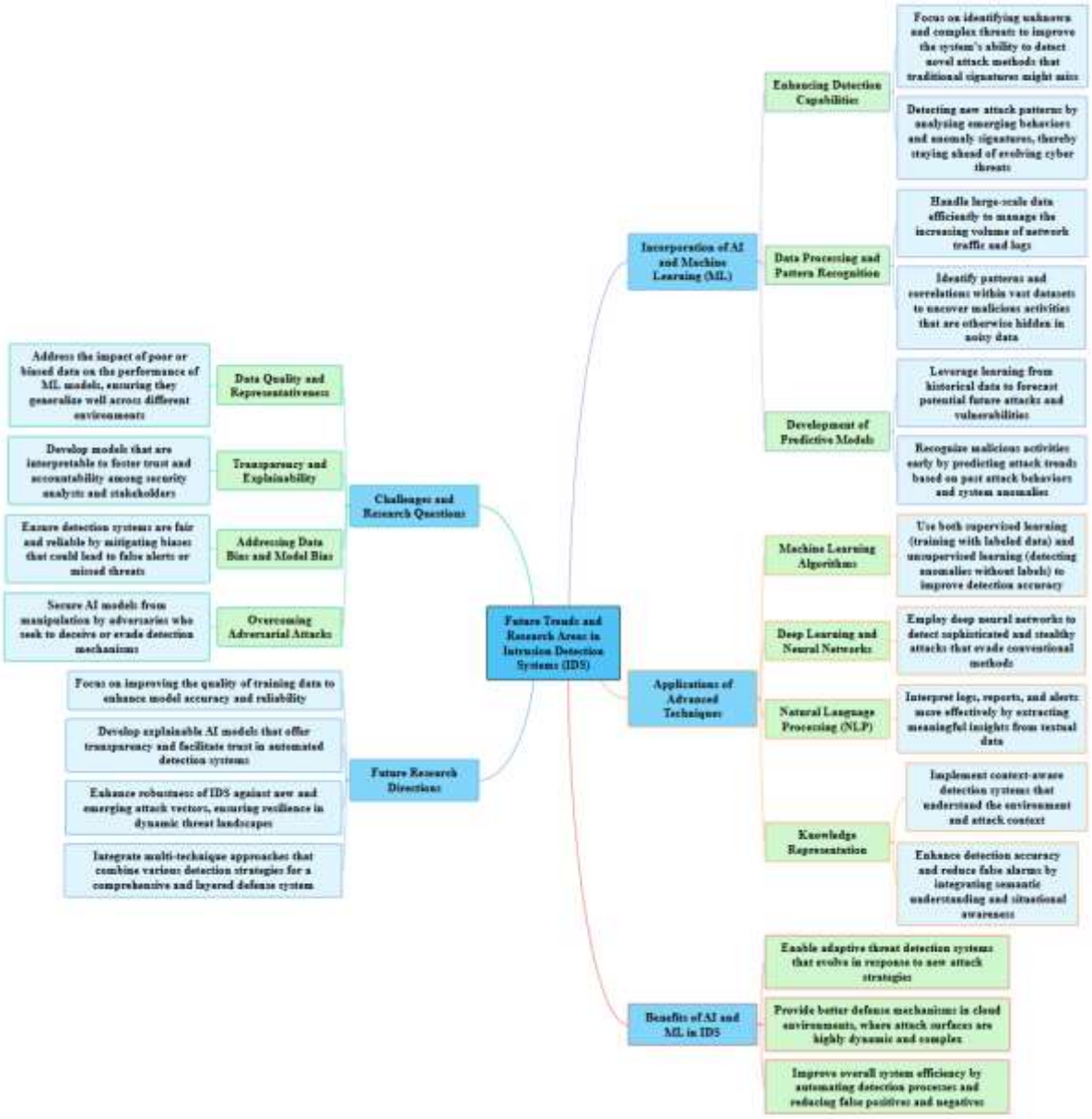

Figure 6. Future Trends and Research Directions.

10.2. Contributions and Implications

The review provides a comprehensive overview of the IDS in cloud computing and IoT, offering valuable insights for researchers and practitioners to develop effective solutions. It contrasts current methods of IDS, points out the future research directions, and stresses how they can improve security in dynamic settings. The results can be applied to academic and industrial settings to advance the creation of new IDS technologies and educate users on improved deployment and management strategies to enhance cloud and IoT security.

References

1. S. Singh, K. Saxena, and Z. Khan. Intrusion detection based on artificial intelligence techniques. In Proceedings of the International Conference of Advanced Research and Innovation, Icari, 2014.
2. S. Prakash. Role of virtualization techniques in a cloud computing environment. In Advances in Computer Communication and Computational Sciences. Springer, Singapore, 2019.
3. M. R. Feizi-Derakhshi, M. M. Alhusseini, Hassan S. Ahmed, AI-based IDS: A Novel Hybrid Intrusion Detection System (HyIDS) based on MLP and LSTM Optimized by the Combination of the Energy Valley

 doi:10.20944/preprints202603.1817.v1

Optimizer and Snake Optimizer Algorithm, Iraqi Journal for Computer Science and Mathematics (under review), 2025

4. M. Rana and J. Singla. A systematic review on data mining rules generation optimization via genetic algorithm. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC), 2020.
5. M. Idhammad, K. Afdel, and M. Belouch. Detection system of HTTP DDoS attacks in a cloud environment based on information-theoretic entropy and random forest. Security and Communication Networks, 1263123, 2018.
6. P. S. Bawa, S. U. Rehman, and S. Manickam. Enhanced mechanism to detect and mitigate economic denial of sustainability (EDoS) attack in cloud computing environments. International Journal of Advanced Computer Science and Applications, 8(9):51–58, 2017.
7. V. Jyothsna and V. V. Rama Prasad. Fcaais: anomaly-based network intrusion detection through feature correlation analysis and association impact scale. ICT Express, 2(3):103–116, 2016.
8. D. Y. Yeung and Y. Ding. Host-based intrusion detection using dynamic and static behavioral models. Pattern Recognition, 36(1):229–243, 2023.
9. K. Vieira, A. Schulter, C. Westphall, and C. Westphall. Intrusion detection techniques in grid and cloud computing environments. IEEE IT Professional Magazine, 12, 2010.
10. A. Kumar, A. Viinikainen, and T. Hamalainen. Machine learning classification model for a network-based intrusion detection system. In Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST), pages 242–249, Barcelona, Spain, 2016.
11. A. H. Bhat, S. Patra, and D. Jena. Machine learning approach for intrusion detection on cloud virtual machines. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(6):57–66, 2013.
12. Y. Yang, S. Tu, R. H. Ali, H. Alasmary, M. Waqas, and M. N. Amjad. Intrusion detection based on bidirectional long short-term memory with an attention mechanism. 2023.
13. H. Saini, Y. Shankar Rao, and Tarini Charan Panda. Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2):202–209, 2012.
14. H. Lin, Q. Xue, J. Feng, and Di Bai. An Internet of Things intrusion detection model and algorithm based on cloud computing and multi-feature extraction, an extreme learning machine. Digital Communications and Networks, 9(1):111–124, 2023.
15. M. Dikaiakos, G. Pallis, D. Katsaros, P. Mehra, and A. Vakali. Cloud computing: Distributed internet computing for it and scientific research. IEEE Internet Computing, 2009.
16. P. Kalagiakos and P. Karampelas. Cloud computing learning. IEEE, pages 7–11, 2011.
17. P. Mell and T. Grance. The NIST definition of cloud computing. National Institute of Standards and Technology - Computer Security Resource Center, 2011.
18. Y. Sahu and RK Pateriya. Cloud computing overview with load balancing techniques. International Journal of Computer Applications, 65(24):40–44, 2013.
19. K. Kaur, A. Singh, and A. Sharma. A systematic review on resource provisioning in fog computing. Transactions on Emerging Telecommunications Technologies, page e4731, 2023.
20. S. Ahmad, S. Mehfuz, and J. Beg. Assessment of potential security threats and introducing a novel data security model in a cloud environment. Materials Today: Proceedings, 2022.
21. R. Helaimia. Cloud computing in higher education institutions: Pros and cons. International Journal of Advanced Natural Sciences and Engineering Research, 7(3):132–141, 2023.
22. L. Golightly, V. Chang, Q. Ariel Xu, X. Gao, and B. SC Liu. Adoption of cloud computing as an innovation in the organization. International Journal of Engineering Business Management, 14, 2022.
23. M. Sharifzadeha, H. Malekpoura, and Ehsan Shojab. Cloud computing and its impact on Industry 4.0: An overview. Industry 4.0 Vision for Energy and Materials: Enabling Technologies and Case Studies, pages 99–120, 2022.
24. G. Fortino, A. Guerrieri, C. Savaglio, and G. Spezzano. A review of Internet of Things platforms through the IoT-A reference architecture. Intelligent Distributed Computing XIV, pages 25–34, 2022.

 doi:10.20944/preprints202603.1817.v1

25. S. Narang and S. Kumar. Application of virtualization in cloud computing. Eduzone: International Peer-Reviewed/Refereed Multidisciplinary Journal, 11(2):106–111, 2022.
26. N. Azeez, T. M. Bada, S. Misra, A. Adewumi, C. V. Vyver, and R. Ahuja. Intrusion detection and prevention systems: an updated review. Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1, pages 685–696, 2020.
27. V. P. Gandi, N. S. Lalith, G. Sadhineni, S. Geddamuri, G. K. Chaitanya, and AK Velmurugan. A comparative study of ai algorithms for anomaly-based intrusion detection. In 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), pages 530–534. IEEE, 2023.
28. E Dritsas, M Trigka, A survey on the applications of cloud computing in the industrial Internet of things, Big data and cognitive computing, Feb 17;9(2):44, 2025
29. A. Mijuskovic, A. Chiumento, R. Bemthuis, A. Aldea, and P. Havinga. Resource management techniques for cloud/fog and edge computing: An evaluation framework and classification. Sensors, 21(5):1832, 2021.
30. D Rupanetti, N Kaabouch, combining edge computing-assisted internet of things security with artificial intelligence: Applications, challenges, and opportunities, Applied Sciences. Aug 13;14(16):7104., 2024
31. M. Otair, O. T. Ibrahim, L. Abualigah, M. Altalhi, and P. Sumari. An enhanced grey wolf optimizer-based particle swarm optimizer for intrusion detection systems in wireless sensor networks. Wireless Networks, 28(2):721–744, 2022.
32. N. Omer, A. H. Samak, A. I Taloba, and Rasha M Abd El-Aziz. A novel optimized probabilistic neural network approach for intrusion detection and categorization. Alexandria Engineering Journal, 72:351–361, 2023.
33. A. Heidari and M. A. Jamali. Internet of things intrusion detection systems: A comprehensive review and future directions. Cluster Computing, pages 1–28, 2022.
34. M. Muhammad and A. Saleem. An intelligent intrusion detection system for the Apache web server empowered with machine learning approaches. International Journal of Computational and Innovative Sciences, 1(1):1–8, 2022.
35. J. Verdejo, J. Muñoz-Calle, A. E. Alonso, Rafael Estepa Alonso, and Germán Madinabeitia. On the detection capabilities of signature-based intrusion detection systems in the context of web attacks. Applied Sciences, 12(2):852, 2022.
36. T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. Ali Bahaj. Anomaly-based intrusion detection system for IoT networks through a deep learning model. Computers and Electrical Engineering, 99:107810, 2022.
37. S. Alem, D. Espes, L. Nana, E. Martin, and F. De Lamotte. A novel bi-anomaly-based intrusion detection system approach for Industry 4.0. Future Generation Computer Systems, 2023.
38. N. Mishra and S. Pandya. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9:59353– 59377, 2021.
39. D. Theng and S. Golait. A review of intrusion detection techniques for cloud computing and security challenges. 02 2015.
40. Y. Alghofaili, A. Albattah, N. Alrajeh, M. A Rassam, and B. Ali Saleh Alrimy. Secure cloud infrastructure: a survey on issues, current solutions, and open challenges. Applied Sciences, 11(19):9005, 2021.
41. A. Khraisat and A. Alazab. A critical review of intrusion detection systems in the Internet of Things: techniques, deployment strategy, validation strategy, attacks, public datasets, and challenges. Cybersecurity, 4:1–27, 2021.
42. JK Samriya, S Kumar, M Kumar, M Xu, H Wu, SS Gill, Blockchain and reinforcement neural network for trusted cloud-enabled IoT network. IEEE Transactions on Consumer Electronics, 70(1), pp.2311-2322, 2023
43. A. Thakkar and R. Lohiya. A survey on intrusion detection systems: feature selection, model, performance measures, application perspectives, challenges, and future research directions. Artificial Intelligence Review, 55(1):453–563, 2022.
44. A. Hayajneh, M. Z. Alam Bhuiyan, and I. McAndrew. Improving Internet of Things (IoT) security with Software-Defined Networking (SDN). Computers, 9(1):8, 2020.
45. KF Ystgaard, L Atzori, D Palma, PE Heegaard. Review of the theory, principles, and design requirements of human-centric Internet of Things (IoT). Journal of Ambient Intelligence and Humanized Computing. Mar;14(3):2827-59. 2023

 doi:10.20944/preprints202603.1817.v1

46. B Xu, L Sun, X Mao, R Ding, C Liu, IoT intrusion detection system based on machine learning. Electronics. Oct 17;12(20):4289, 2023
47. M. M. Rahman, S Al Shakil, MR Mustakim, A survey on intrusion detection systems in IoT networks, Cyber Security and Applications. Dec 1; 3:100082, 2025
48. C Saadouni, S El Jaouhari, N Tamani, Identification techniques in the Internet of things: Survey, taxonomy and research frontier, IEEE Communications Surveys & Tutorials. Feb 11, 2025
49. M Kumar. Deep learning approach for intrusion detection system (IDS) in the Internet of Things (IoT) network using gated recurrent neural networks (GRU), 2017.
50. AA Diro and N Chilamkurti. Distributed attack detection scheme using a deep learning approach for the Internet of Things. Future Generation Computer Systems, 82:761–768, 2018.
51. M Roopak, GY Tian, and J Chambers. Deep learning models for cybersecurity in IoT networks. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pages 452–457. IEEE, 2019.
52. G Thamilarasu and S Chawla. Towards deep-learning driven intrusion detection for the Internet of things. Sensors, 19(9):1977, 2019.
53. Y. Otoum, D. Liu, and A. Nayak. Dl-ids: a deep learning-based intrusion detection framework for securing iot. Transactions on Emerging Telecommunications Technologies, 30(12):e3803, 2019.
54. S Pande, A Khamparia, D Gupta, and DNH Thanh. DDoS detection using a machine learning technique. In Recent Studies on Computational Intelligence. Studies in Computational Intelligence, volume 921, pages 1–13. Springer, Singapore, New Delhi, 2021.
55. S Pande, A Khamparia, and D Gupta. An intrusion detection system for a healthcare system using machine and deep learning. World Journal of Engineering, 2021.
56. G Bovenzi, G Aceto, D Ciuonzo, V Persico, and A Pescapé. A hierarchical hybrid intrusion detection approach in iot scenarios. In GLOBECOM IEEE Global Communications Conference, pages 1–7. IEEE, 2020.
57. Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa, and B. A Al-rimy. Deepiot.ids: hybrid deep learning for enhancing IoT network intrusion detection. CMC-Computers, Materials & Continua, 69(3):3945–3966, 2021.
58. F. A. Fadhil, M. M. Alhusseini, and M. R. Feizi-Derakhshi, Enhanced cast-128 with adaptive s-box optimization via neural networks for image protection, In 4th International Conference on Advanced Engineering, Technology and Applications on Power Systems, Online, 31-July-2025
59. W. Hassan, T. Chou, L. Pagliari, J. Pickard, and O. Tamer. Is public cloud computing adoption strategically the way to go for all enterprises? In IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), 2019.
60. J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. Raymond Choo. Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. ACM Computing Surveys (CSUR), 54(8):1–36, 2021.
61. E. M. Onyema, S. Dalal, C. A. Romero, B. Seth, P. Young, and M. A. Wajid. Design of an intrusion detection system based on cyborg intelligence for the security of cloud network traffic of smart cities. Journal of Cloud Computing, 11(1):1–20, 2022.
62. M. M. Alhusseini, A. Rouhi, A Novel Hybrid Intrusion Detection Model: A New Metaheuristic Approach for Feature Selection Based on AI Techniques for Cyber Threat Detection. Iraqi Journal for Computer Science and Mathematics 6(4):4. 2025.
63. F. A. Fadhil, FTA Hussien Alhilo, MT Abdulhadi, Enhancing data security using Laplacian of Gaussian and ChaCha20 encryption algorithm, Journal of Intelligent Systems. Sep 5;33(1):20240191, 2024
64. H. Liu and Bo Lang. Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences, 9(20):4396, 2019.
65. I. Butun, A. Sari, and P. Österberg. Security Implications of Fog Computing in the Internet of Things. In IEEE International Conference on Consumer Electronics (ICCE), pages 1–6. IEEE, 2019.
66. H. Bakır, Ö Ceviz, Empirical enhancement of intrusion detection systems: a comprehensive approach with genetic algorithm-based hyperparameter tuning and hybrid feature selection, Arabian Journal for Science and Engineering. Sep;49(9):13025-43, 2024

 doi:10.20944/preprints202603.1817.v1

67. QM Alzubi, SN Makhadmeh, Y Sanjalawe, Optimizing Intrusion Detection: Advanced Feature Selection and Machine Learning, Techniques Using the CSE-CIC-IDS2018 Dataset, Journal of Advances in Information Technology;16(3), 2025
68. A. M. Alsaffar, M Nouri-Baygi, HM Zolbanin, shielding networks: enhancing intrusion detection with hybrid feature selection and stack ensemble learning, Journal of Big Data. Sep 18;11(1):133, 2024
69. M. Alsheikh, L. Konieczny, M. Prater, G. Smith, and S. Uludag. The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. IEEE Consumer Electronics Magazine, 11(3):59–68, 2021.