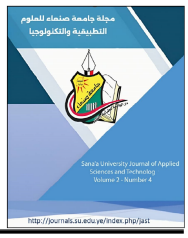
Vol.2, No.4, Page 363- 374, 2024 https://doi.org/10.59628/jast.v2i4.970 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/



Survey of Intrusion Detection Techniques in Cloud Computing

Suad Mohammed Othman[1] *, Adnan Yehia Al-mutawkkil[1] and Amani Mohammed Alnashi[2]

[1]**Department of Information Technology, Faculty of Computer IT, University of Sana'a, Sana'a, Yemen,**
[2]**Department of Information System, Faculty of Computer & IT, University of Sana'a, Sana'a, Yemen**

*Corresponding author: Suad.m.othman@gmail.com

Abstract

With the continued development of cloud computing environments, security measures have become more important than ever. Intrusion detection systems (IDS) are considered one of the most critical security measures in cloud computing. Researchers aim to find effective technologies for detecting intrusions in cloud computing. This paper presents a comprehensive survey of the techniques used for Intrusion Detection in Cloud Computing and their classification. Specifically, it covers a range of techniques such as machine learning, and provides insights for researchers looking to develop more flexible and effective techniques for intrusion detection in cloud computing.

Article Info

Keywords:
Intrusion Detection, Cloud Computing, Security, Classification, Techniques, Cyber Threats

Article History:
Received: 27-April-2024,
Revised: 22-July-2024,
Accepted: 18-August-2024,
Available online: 30 August 2024.

1. INTRODUCTION

Cloud computing is becoming increasingly popular in computer science and is often described as a new data hosting technology. This technology has gained popularity due to the cost benefits it offers businesses. Cloud computing plays a crucial role in computer science and is rapidly contributing to its development. The National Institute of Standards and Technology (NIST) defines cloud computing as a model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, services, etc.). These resources can be rapidly allocated and freed up with minimal management effort or need for service provider involvement. According to S Dixit, G Hussain [1], cloud computing can be defined as a method for sharing resources more efficiently with clients. It relies on the concept of virtualization, and there are various types of service models including IaaS, PaaS, and SaaS. **Cloud computing** is a modern technology that provides shared computing resources over the internet to manage, retrieve, and store data. Cloud computing (CC) can deliver service models such as platforms, software, and infrastructure based on customer needs and usage. The virtualization of storage resources and their applications is a fundamental requirement of cloud computing [2]. Cloud computing is emerging as a powerful solution to meet the growing storage and processing needs of organizations and individuals without the burden of owning and managing physical devices [3]. It is offered as a response to user demands to reduce overall costs and complexity. It is gaining popularity due to its various advantages such as on-demand services, flexible resource allocation, high fault tolerance, and high scalability [4]. Challenges in cloud computing include security, privacy, cost, load balancing, and performance management. Among these challenges, security is paramount since user data and applications reside in the cloud [5]. Vashishtha [6][6] explained the different types of attacks in cloud computing, which we will discuss in the following section.

1.1. Attacks on Cloud Computing

Cloud computing faces significant challenges related to security and the data stored on cloud servers. The primary concern in cloud computing is ensuring security. According to Vashishtha [6], there are many types of attacks in cloud computing that we can summarize as follows:

- **Denial of Service (DoS) Attack**:An attacker uses an innocent network host or computer to send a large number of packets to a victim [7]. These bogus packets consume most of the bandwidth, preventing new connections from being established. This makes the service unavailable to authorized users [8].
- **User-to-Root Attack**:An intruder attempts to gain control of an authentic user's account by spying on their password. Using this technique, an attacker can gain root access to the system and alter all critical data [9].
- **Insider Attack**:In this attack, an authorized user attempts to disclose data using unauthorized privileges.
- **Port Scanning**: The attacker scans for open ports on the victim's machine. They use a port scanner to create a list of closed, open, and filtered ports, then exploit these ports to attack and disrupt services used by real users.
- **Hypervisor Attacks / Virtual Machine Attacks**:By exploiting vulnerabilities in the hypervisor, an attacker can gain control of the installed virtual machine (VM). These attacks allow attackers to take control of systems and hosts by attacking installed hypervisors.
- **Backdoor Channel Attacks**: Backdoors in a compromised computer can be used by hackers to gain remote access to the system. Hackers can use backdoors to install malware and steal data from your system or network.
- **Routing Information Protocol Attacks**:An attacker obtains routing information from trusted peer routers and manipulates or corrupts the routing data. This occurs when a malicious user modifies the routing table, causing abnormal network traffic.
- **Tunnel Attack**:This attack aims to bypass firewall filters. Firewalls filter network traffic according to network protocol data. Attackers use application layer mining attacks to exploit application vulnerabilities by delivering packets directly to these programs.

Due to the distributed and open architecture of cloud computing, many types of attacks exist. Therefore, it is essential to have mechanisms in place to detect and prevent these attacks. An intrusion detection system plays a crucial role in protecting a computer system from such threats.

1.2. Intrusion detection system

The Intrusion Detection System (IDS) monitors network traffic for suspicious activity and alerts the system or network administrator if any irregularities are detected. Alerts are raised when user actions significantly deviate from standard behavior or match known threat signatures. Incomplete or incorrect interpretation of behavior or signatures can result in false positives or false negatives. A false positive occurs when legitimate behavior is mistakenly flagged as malicious [10]. IDSs come in various types and employ different methods to detect suspicious traffic. They can be network-based or host-based. Some IDSs detect threats by looking for specific signatures of known threats, while others use a baseline of normal behavior to identify anomalies. A signature-based IDS examines packets on the network and compares them against a database of known malicious signatures. One challenge with this method is the delay between the discovery of a new threat and the update of the signature database, during which the IDS cannot detect the new threat. An anomaly-based IDS continuously monitors network traffic, comparing it to a predefined baseline that identifies normal behavior for that network. When traffic deviates significantly from this baseline, the IDS alerts the administrator or user. The main goals of an IDS include monitoring access and detecting irregular access or attacks on the system. In machine learning, a key task is to identify anomalies in data. These techniques are used to detect both known and unknown attacks in the cloud environment. Implementing intrusion detection systems in cloud computing environments comes with a set of challenges and difficulties. Here are some of the main challenges:

1 **Multi-tenancy** Multi-tenancy: In cloud computing environments, data from multiple clients is hosted on the same infrastructure. This can complicate the distinction between legitimate and malicious activity.
Difficulty:Ensuring complete isolation between tenants and guaranteeing data privacy and security for each tenant can be difficult.

2 **Elasticity and Scalability** Cloud computing is characterized by highelasticity, where resources can change rapidly.
Difficulty: Intrusion detection systems need to adapt to rapid changes in scale and resources, which can be challenging to implement.

3 **Data Encryption** Data stored and transmitted in the cloud is often encrypted.
Difficulty: Encryption can make it difficult for intrusion detection systems to effectively analyze data for threats.

4 **Virtualization Technologies** Cloud computing heavily relies on virtualization technologies like virtual machines and containers.
Difficulty: These technologies add a layer of complex-

ity as intrusion detection systems must handle traffic between virtual machines and monitor activities within them.

5 **Lack of Visibility and Control** In cloud environments, full control and detailed visibility of the infrastructure are often in the hands of the cloud service provider, not the client.
Difficulty: This reduces the ability to effectively implement and monitor intrusion detection systems.

6 **Integration with Diverse Systems** Cloud computing environments consist of diverse components and systems.
Difficulty: Achieving integration between intrusion detection systems and all these different components can be complex and require significant effort.

7 **Alert Management** Intrusion detection systems generate large volumes of alerts.
Difficulty: The high number of alerts can overwhelm security teams, making it hard to distinguish between false positives and real threats.

8 **Compliance and Regulations** Cloud environments must comply with various regulatory and compliance requirements.
Difficulty: Achieving compliance while maintaining the performance of the intrusion detection system can be a significant challenge.

9 **Evolving Threats** Security threats are constantly evolving.
Difficulty: Intrusion detection systems need continuous updates to keep up with new threats, requiring significant resources and effort.

Addressing these challenges requires a comprehensive strategy and techniques that include using advanced tools and technologies, close collaboration with cloud service providers, and continuous training for security teams on the latest threats and protection methods. In this paper, we introduce, review, and classify different techniques used for IDS in cloud computing

2. RELATED WORK

Many research papers have provided an overview of the techniques used in intrusion detection. In this section, we summarize some of these works: This paper [11] provided an overview of various aspects to consider in machine learning intrusion detection systems. In this study, an intrusion detection system was introduced, discussing classification types, the attacks they faced, and the organization of security incident response infrastructure. The study also explained that several studies on intrusion detection using machine learning detailed the databases used. This study [12] conducted a systematic literature review focusing on anomaly-based intrusion detection methods, particularly for detecting insider attacks. It aimed to enumerate techniques for modeling host-based and network-based anomaly detection. The researcher focused on insider attacks only, which limited the comprehensiveness of the study regarding external attacks or other threats. Additionally, the methods used were not compatible with the latest developments and technologies in cybersecurity and cloud computing. This research [5] provided a comprehensive overview of existing security technologies, detailing their strengths and weaknesses. It addressed security concerns in any cloud service model, the importance of feature selection and dimensionality reduction, and the state of IDS technologies. The study categorized IDS techniques based on identified attacks, their deployment, and configuration. Despite offering a comprehensive overview, the research lacked practical applications and specific implementation recommendations for security in actual cloud environments. Furthermore, the significant focus on feature selection and dimensionality reduction might have overlooked other important aspects of security. This paper [13] presented a systematic literature review of intrusion detection systems in cloud-based IoT environments. It systematically examined key articles and essential techniques in this domain. In cloud-based IoT IDSs, they were categorized into three major types: learning-based, pattern-based, and rule-based mechanisms, highlighting the main challenge of IDS, which was precision and detection. The researcher classified intrusion detection systems into only three types, which were limited by the type of attacks and modern techniques, making the research less comprehensive for other classifications by various criteria. In addition, the low accuracy in intrusion detection indicated the lack of effective solutions to overcome this problem. This article [4] analyzed four intrusion detection systems for detecting attacks. Additionally, it highlighted the growing challenges of securing sensitive user data and provided useful recommendations to address the identified issues. The researcher analyzed only four intrusion detection systems, which made the analysis insufficient to provide a comprehensive view of all possible systems. The authors [3] comprehensively studied different intrusion detection and prevention (IDP) techniques and analyzed their respective strengths and weaknesses across various parameters to ensure security in cloud computing. In this study, the analysis lacked case studies or real-world data to support the findings and theories presented. The focus on strengths and weaknesses may have ignored the practical aspects of integrating these technologies with existing cloud computing systems. In this study, we provided a comprehensive classification of the techniques used in intrusion detection, including the latest techniques used in cloud computing. We also discussed a case study as a practical application of using intrusion detection in cloud computing. In the section below, we presented the techniques in detail with some research on each technique, comparing the techniques in terms of advantages and disadvantages, and when to

use them as shown in figure 1.

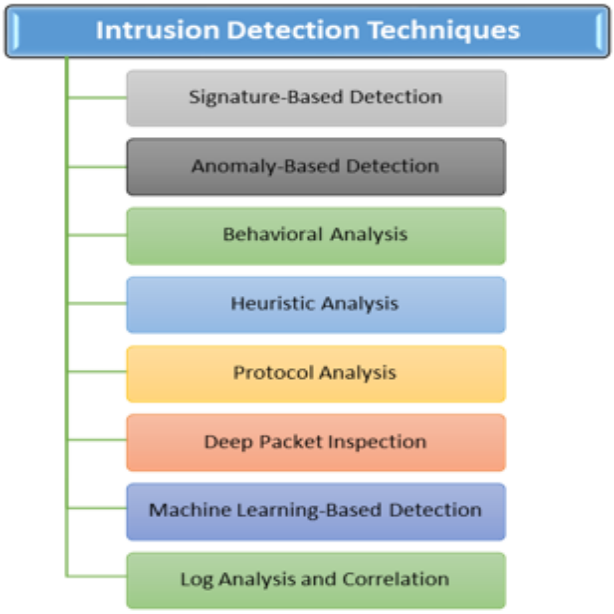


Figure 1. Classification of IDS techniques in cloud computing.

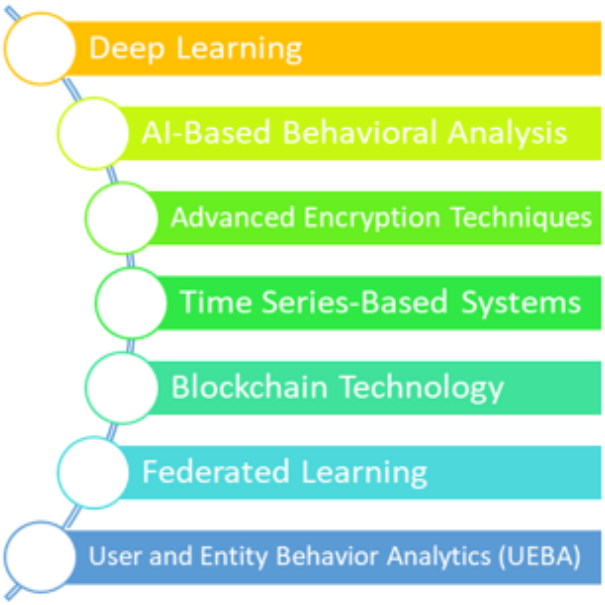


Figure 2. Classification of IDS modern techniques in cloud computing.

3. SIGNATURE-BASED DETECTION

Signature-based detection is a method used in cybersecurity to identify and block known malicious activities and threats. It uses predefined patterns or signatures that represent characteristics of known malware, viruses, or other types of malicious code. H. Asad [14] stated that a signature-based approach utilizes a database containing traffic signatures, including port numbers, IP addresses, protocols, and payload patterns. It generates alerts when it detects matching signatures.

4. ANOMALY-BASED DETECTION

Anomaly-based detection is an approach that focuses on identifying deviations from normal operations within a system or network. Instead of relying on predefined signatures of known threats, anomaly-based detection attempts to identify anomalies or activities that are inconsistent with recognized patterns of behavior. The authors [15] developed an Intrusion Detection System using Pearson-Correlation Coefficient and Convolutional Neural Networks to detect network anomalies. This system performed binary classification and multiclass classification. The approach proposed by the authors [16] combined two types of Intrusion Detection Systems using Neural Networks through a Decision-Making System. This type of Intrusion Detection System includes two additional sub-categories: specification-based and behavioral-based IDS [17], as shown in Figure 3.

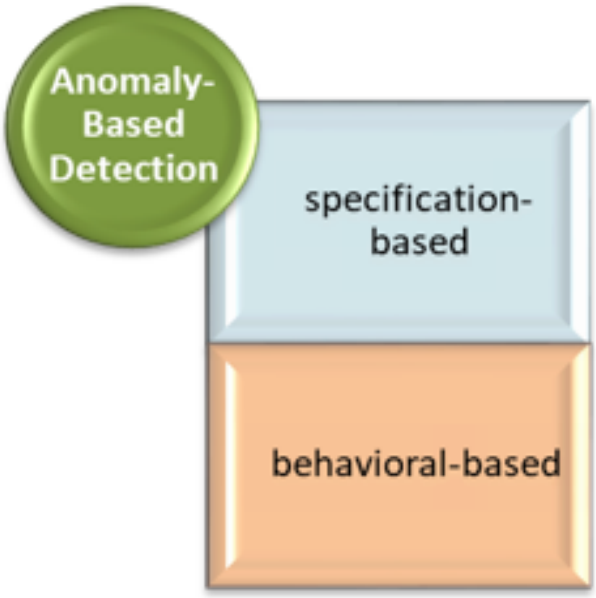


Figure 3. Anomaly detection types.

5. BEHAVIORAL ANALYSIS

Behavioral analysis in intrusion detection is a technique that monitors and analyzes system, network, or user behavior to identify abnormal activity that may indicate a threat. This approach involves understanding typical behavior patterns within a network or system and identifying deviations from normal behavior. The authors [17] proposed a new approach to user behavior analysis on networks using swarm intelligence algorithms. This approach involved creating a swarm of agents to represent users on the network and using simple rules to

govern the agents interactions with each other and the environment.

6. HEURISTIC ANALYSIS

Heuristic analysis is a technique where general rules and guidelines are applied to identify previously unknown or novel threats based on their characteristics and behavior. Key phases of protocol analysis in intrusion detection are shown in Figure 4.

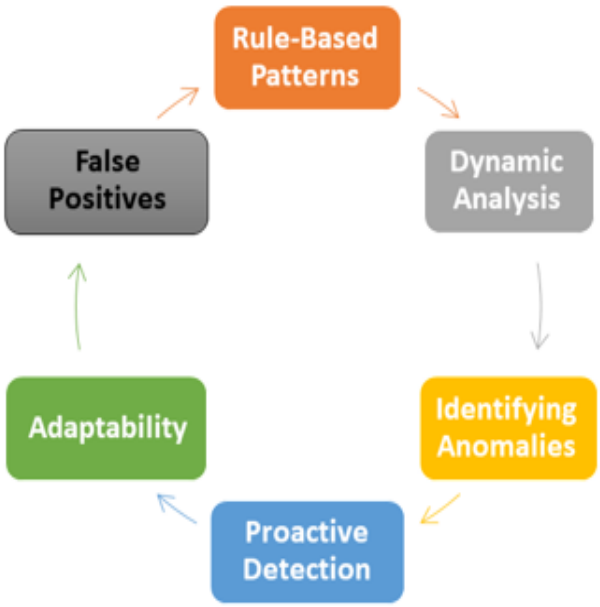


Figure 4. key aspect of Heuristic analysis

1) **Rule-Based Patterns**:Creating and applying rules or heuristics that represent common characteristics of known threats. These rules are typically designed to detect patterns and behaviors that indicate malicious activity [18].
2) **Dynamic Analysis**:Examines code or files without executing them. Heuristic analysis often involves dynamic analysis, which observes the behavior of software or system components while they are running.
3) **Identifying Anomalies**:Heuristics are used to identify anomalies or deviations from expected behavior. Rather than relying on specific signatures, heuristic analysis looks for patterns that may indicate malicious intent.
4) **Proactive Detection**:Heuristic analysis is considered a proactive detection method because it does not rely on known signatures. The goal is to detect new threats by identifying patterns and behaviors that deviate from normal activity.
5) **Adaptability**:Because heuristic analysis is not based on existing signatures, it can adapt to new and evolving threats. As cyber threats change, heuristics can be updated to account for new attack vectors.
6) **False Positives**:A challenge in heuristic analysis is the possibility of false positives. Because they rely on common rules, they run the risk of misinterpreting legitimate activity as malicious.

7. PROTOCOL ANALYSIS

Protocol analysis is the examination and monitoring of network communication protocols to identify malicious activities. This technique involves inspecting the headers and content of network packets to detect anomalies or deviations from expected behaviors [19]. The goal is to identify potential security threats, attacks, or unauthorized activities within a network. Key phases of protocol analysis in intrusion detection are shown in Figure 5.

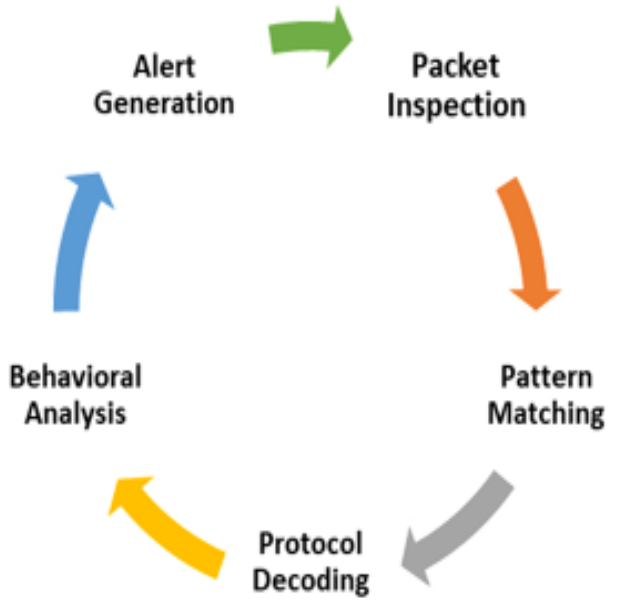


Figure 5. Phases of protocol analysis

1. **Packet Inspection**:Inspects the contents of network packets to analyze communications between devices on the network. This involves examining the packet header to understand the details of the communication.
2. **Pattern Matching**:Uses predefined patterns to identify known attack patterns within network traffic. These patterns may include particular byte sequences or characteristics associated with common network-based attacks.
3. **Protocol Decoding**:Understands and decodes various network protocols such as TCP/IP, HTTP, and UDP. By decoding these protocols, security systems can analyze the structure and content of network communications.
4. **Behavioral Analysis**:Observes the behavior of network protocols to identify expected deviations from standards. Unusual or suspicious communication patterns can indicate a potential security incident.
5. **Generate Alerts**:Generates alerts when suspi-

cious activity is detected. These alerts can be used to prompt further investigation by security administrators or automated response systems.

The authors [20] proposed a protocol-based Intrusion Detection System (IDS) specifically for HTTP. This IDS provides real-time intrusion detection and generates web log-based alerts, notifying the admin immediately if any suspicious activity is detected in the weblog.

8. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) is a monitoring technology that involves examining and analyzing the content of data packets at a deep level within a network [21]. DPI goes beyond traditional packet filtering, which typically involves looking at header information such as source and destination addresses or ports. DPI examines the actual content of the packets to gain insights into the nature of the traffic. Commonly used protocols for DPI include sFlow, NetFlow, and IPFIX for flow-based analysis. There are many datasets used in DPI, such as the dataset introduced by authors [22] for deep packet inspection and analysis. The components of DPI are shown in Figure 6.

1. **Packet Capture**: DPI captures and logs individual data packets as they cross the network.

2. **Packet Analysis**: The content of each packet is analyzed in-depth, including payload inspection and examination of application-layer protocols.

3. **Signature Matching**: DPI uses predefined signatures or patterns to identify known threats or specific types of content.

4. **Heuristic Analysis**: Some DPI solutions use heuristics to identify patterns indicative of anomalous behavior.

5. **Protocol Decoding**: DPI can decode and analyze various network protocols, including application-layer protocols such as HTTP, SMTP, and more.

The authors [23] introduced a new data structure and used it as a tool for matching checks in DPI. It is called the Dual Cuckoo Filter.

9. MACHINE LEARNING-BASED DETECTION AND DEEP LEARNING

Machine learning models can be trained to differentiate between normal and malicious behavior. Machine learning, especially deep learning, has become a popular technique for developing solutions to detect malware [24]. This research paper [25] proposed an intrusion detection system that combines optimization and boosting techniques to classify and detect malware-related records in innovative health app platforms. The authors used particle swarm optimization and AdaBoost algorithms as classifiers. The authors proposed [26] suggested a machine learning approach for identifying DDoS attacks in IoT networks using the random forest algorithm. The authors [27] created and implemented a neural network model for detecting intrusions in computer networks, using sampling techniques to address data imbalance in the CICIDS 2017 dataset.

Figure 6. Components of DPI

10. LOG ANALYSIS AND CORRELATION

Log analysis is a technique for extracting insights from log files that contain records of events occurring in a computer system [28]. Logs capture information about events, activities, and errors, and provide a sequential record of system and network activity. The log analysis process [29] is shown in Figure 7.

1. **Collection**: Collect log data from various sources within the IT infrastructure.
2. **Normalization**: Converts log entries into a standardized format for consistency.
3. **Parsing**: Extracts relevant information from log entries [30].
4. **Analytics**: Identifies patterns, anomalies, or suspicious activity.
5. **Alerts**: Generates alerts about security incidents or potential threats.

Log correlation correlates information from different log sources to provide a comprehensive view of an event or set of events. By combining data from multiple protocols, correlations can reveal relationships and dependencies that are not obvious when examining the protocols alone. The authors [31] introduced AMiner, an open-source

tool within the AECID toolbox, which facilitates rapid log parsing, analysis, and alerting. In this paper [32], the authors proposed a novel unsupervised method that autonomously analyzes variable parts of log lines to detect anomalies.

Figure 7. Log analysis process.

11. DEEP LEARNING

One branch of machine learning that can produce excellent outcomes is deep learning. Jakhar and Kaur define deep learning as a subset of machine learning that is used in computational problem-solving through models and algorithms that mimic the biological neural networks of the brain. Like the brain, deep learning works by interpreting information, classifying it, and assigning it to various categories [33, 34]. There are numerous deep learning models that are widely discussed and utilized in various contexts, such as cloud computing and targeted attack scenarios like distributed denial of service (DDoS) attacks. These models include convolutional neural networks, deep belief networks, autoencoders, deep neural networks, recurrent neural networks, and self-normalizing neural networks [34].

12. AI-BASED BEHAVIORAL ANALYSIS

AI-based behavioral analysis employs artificial intelligence techniques to analyze patterns of human or machine behavior to detect anomalous or malicious activities. These techniques include machine learning and deep learning, which are used to create models that can distinguish between normal and abnormal behavior based on historical data [35].

13. ADVANCED ENCRYPTION TECHNIQUES

Advanced encryption techniques play a critical role in securing cloud computing environments by protecting data integrity, confidentiality, and authenticity. These techniques help in safeguarding data against unauthorized access and malicious activities, which are vital in intrusion detection systems (IDS). Here's an overview of some advanced encryption techniques and their application in intrusion detection for cloud computing:

1. **Homomorphic Encryption**: Allows computations to be performed on encrypted data without needing to decrypt it first. It is useful in cloud computing as it ensures that data remains encrypted even during processing, providing a high level of security. In a study by Li et al. [36], homomorphic encryption was utilized to create a privacy-preserving IDS for cloud environments. The encrypted data could be analyzed for intrusion without exposing the raw data, ensuring privacy and security.
2. **Attribute Based Encryption (ABE)**: A form of public-key encryption where the secret key of a user and the ciphertext are dependent upon attributes (e.g., user roles or characteristics). It enhances access control in cloud environments, ensuring that only authorized users can decrypt and access specific data. In a study by [37], this technique was explored for cloud security.
3. **Quantum Encryption**: Utilizes principles of quantum mechanics to encrypt data, offering theoretically unbreakable encryption. It provides a future-proof method for protecting sensitive data against potential quantum computer attacks. In research by Yang et al., quantum encryption techniques were proposed for securing cloud-based IDS. The study highlighted how quantum keys could be used to secure data transmission and detection processes against sophisticated intrusion attempts.
4. **Blockchain-Based Encryption**: Integrates blockchain technology with encryption to provide decentralized security. It enhances the integrity and traceability of data in cloud environments. A study by Zheng et al. (2020) demonstrated how blockchain combined with advanced encryption techniques could secure IDS in cloud computing. The research showed that this approach could effectively prevent data tampering and ensure secure data sharing across distributed networks.

14. TIME SERIES-BASED SYSTEMS

Time series-based systems have gained prominence in intrusion detection for cloud computing due to their ability to analyze temporal patterns and detect anomalies over time. These systems leverage the sequential nature

of data to identify unusual behaviors that may indicate potential security threats [38]. The study [38] presented a comprehensive methodology for the effective early detection of intrusions in cloud computing based on time series anomalies. By employing a collaborative feature selection model and the Facebook Prophet prediction model, the approach demonstrated significant efficiency and performance improvements.

15. BLOCKCHAIN TECHNOLOGY

Blockchain technology, known for its decentralized and immutable ledger, is being explored for enhancing security in various domains, including intrusion detection systems (IDS). The integration of blockchain with IDS aims to improve the accuracy, transparency, and reliability of detecting intrusions in network systems, including cloud computing environments [39, 40]. The paper presented a novel collaborative framework leveraging blockchain technology to improve the security of IoT networks by overcoming the centralization and scalability issues of traditional IDSs. The proof-of-concept results show that the BC-IDS framework enhances network security and significantly increases scalability [41].

16. FEDERATED LEARNING

Federated Learning (FL) is a decentralized machine learning approach that allows models to be trained collaboratively across multiple devices or servers while keeping the data localized. This technique has garnered significant attention in the context of intrusion detection due to its ability to enhance privacy, scalability, and efficiency [42].

17. USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

User and Entity Behavior Analytics (UEBA) is an advanced security solution that leverages machine learning and analytics to detect anomalies and potential security threats by analyzing the behavior of users and entities within a network. UEBA is particularly effective in cloud computing environments due to its ability to identify subtle and complex threats that traditional security measures might miss [43, 44]. Recent research highlights the effectiveness of UEBA in identifying complex and subtle threats, enhancing cloud security through advanced anomaly detection techniques [45].

18. CLOUD-NATIVE SECURITY SOLUTIONS

Cloud-native security solutions are designed specifically to operate within cloud environments, leveraging the unique capabilities of cloud infrastructure to provide enhanced security measures, including intrusion detection. These solutions take advantage of cloud-native technologies such as microservices, containers, and serverless architectures to detect and respond to security threats more effectively [46]. Recent research underscores the effectiveness of these solutions in addressing the security challenges posed by microservices, containers, and serverless architectures. By integrating automation, orchestration, and machine learning, cloud-native intrusion detection systems offer robust and scalable protection against sophisticated threats [47, 48]. Implementing an Intrusion Detection System (IDS) in cloud computing is crucial for companies that rely on cloud services to store and manage their data. As businesses increasingly move their operations to the cloud, they face many cyber threats that can compromise sensitive information. An IDS plays a vital role in safeguarding this data by continuously monitoring network traffic and system activities for suspicious behavior that could indicate a potential attack. Moreover, an IDS enhances the overall security posture of a company by providing insights into the types of threats it faces. This information can be used to strengthen existing security measures and develop more effective strategies to counter emerging risks. For businesses that use cloud computing, where data is often distributed across multiple locations and accessed by various users, having a robust IDS is essential to ensure their information remains secure. In the following section, we present a case study on the implementation of an intrusion detection system in a company and what it is. Benefits of applying it to the company.

19. CASE STUDY

19.1. Implementing Intrusion Detection Systems in Cloud Computing for XYZ Corporation

Background

XYZ Corporation is a global enterprise that transitioned its IT infrastructure to a cloud-based environment to leverage the benefits of scalability, cost efficiency, and flexibility. With the increasing amount of sensitive data and critical applications hosted in the cloud, ensuring robust security measures became paramount. The company decided to implement an Intrusion Detection System (IDS) to protect its cloud infrastructure from potential threats and unauthorized access.

Objective

The main objective was to deploy an IDS capable of:

- Monitoring network traffic and system activities in real-time.
- Detecting and responding to potential security breaches and anomalies.
- Detecting and responding to potential security breaches and anomalies.

- Ensuring compliance with industry regulations and internal security policies
- Providing detailed logs and reports for forensic analysis and incident response.

Challenges

1. **Multi-Tenancy**: Ensuring data privacy and security for multiple tenants sharing the same cloud infrastructure.
2. **Scalability:** Adapting the IDS to handle the dynamic and scalable nature of the cloud environment.
3. **Visibility**: Achieving comprehensive visibility and control over the cloud infrastructure managed by a third-party provider.
4. **Data Encryption:** Effectively inspecting encrypted data without compromising privacy.
5. **Integration:** Seamlessly integrating the IDS with existing cloud services and applications.

Solution

XYZ Corporation implemented a hybrid IDS solution combining both signature-based and anomaly-based detection techniques to cover a broad spectrum of potential threats.

1. **Deployment:**

- **Network-based IDS (NIDS):** Deployed at key points within the cloud network to monitor traffic flowing in and out of the cloud environment.
- **Host-based IDS (HIDS):** Installed on critical cloud-based servers and virtual machines to monitor system-level activities.

2. **Technologies Used:**

- **Deep Packet Inspection (DPI):** Utilized for thorough analysis of packet contents, helping to detect sophisticated threats.
- **Machine Learning Models:** Trained to distinguish between normal and malicious behaviors, enhancing the IDS's ability to detect zero-day attacks.
- **Log Analysis Tools:** Implemented to collect and analyze logs from various sources, enabling correlation of events and detection of anomalies.

3. **Integration:**

- Integrated the IDS with the cloud service provider's API to gain deeper insights and control over the cloud environment.
- Used orchestration tools to ensure the IDS could scale automatically in response to changes in the cloud infrastructure

4. **Real-Time Alerts and Reports:**

- Configured the IDS to generate real-time alerts and detailed reports on suspicious activities, which were sent to the security operations center (SOC) for immediate action.
- Implemented a dashboard providing a unified view of the security posture, helping administrators quickly identify and respond to threats.

Results

1. Enhanced Security:

- The IDS successfully identified and blocked several intrusion attempts, including DDoS attacks, unauthorized access attempts, and malware infiltrations
- Real-time alerts enabled rapid response, minimizing potential damage and reducing downtime.

2. **Improved Compliance:**

- Achieved compliance with industry standards such as GDPR, HIPAA, and PCI-DSS by maintaining detailed logs and reports for audit purposes.
- The IDS provided the necessary documentation and evidence for regulatory requirements.

3. **Operational Efficiency:**

- Automated scaling of the IDS reduced manual intervention and ensured continuous protection as the cloud environment expanded.
- The integration of machine learning models reduced the number of false positives, allowing the security team to focus on genuine threats.

4. **Visibility and Control:**

- Enhanced visibility into network traffic and system activities across the cloud infrastructure.
- The detailed analysis and correlation of log data provided valuable insights for forensic investigations and incident response.

Implementing an IDS in XYZ Corporation's cloud environment significantly improved the overall security posture, providing robust protection against a wide range of cyber threats. The hybrid approach, combining network-based and host-based IDS with advanced technologies like deep packet inspection and machine learning, proved effective in addressing the unique challenges of cloud security. This case study underscores the importance of tailored IDS solutions in safeguarding cloud infrastructures in today's dynamic and threat-prone landscape.

Table 1. The summarized modern detection techniques

	Strengths	Weaknesses	Usage
Deep learning	Capable of detecting new and unknown threats. Improves performance over time with increased data.	Requires significant computational resources and long training times. May produce false positives if not well-trained.	In environments with large complex data where dynamic pattern recognition is needed
AI-Based Behavioral Analysis	Effective in detecting insider threats and intrusions based on stolen user credentials	Requires a long period to learn normal behavior. May produce false positives if legitimate behavior changes	In organizations where user behavior is the main indicator of potential threats.
Advanced Encryption Techniques	Provides high data security, reducing the chances of tampering or intrusion.	Can be slow and increase resource consumption	In environments that require strong protection for sensitive data.
Time Series-Based Systems	Capable of detecting unusual patterns in system behavior over time.	Can be complex to analyze and requires large historical data sets.	In systems that require constant monitoring and analysis of time-based data changes.
Blockchain Technology	Decentralized system makes tampering difficult. Offers high transparency and traceability.	Can be slow and require significant storage space	In environments that require reliable and tamper-proof records.
Federated Learning	Maintains data privacy and reduces risks of data transfer.	Requires high coordination between different locations and can be complex to implement.	In environments that require data privacy across multiple locations.
User and Entity Behavior Analytics (UEBA)	Effective in identifying insider threats and intrusions based on user behavior.	May produce false positives if legitimate behavior changes.	In organizations where user behavior is the main indicator of potential threats.
Cloud-Native Security Solutions	Provides integrated visibility and monitoring across multiple cloud platforms. Integrates with cloud providers'. tools and APIs	Dependent on the capabilities of the cloud-native security solutions. May require significant investment and integration effort.	In organizations heavily utilizing cloud services.

20. CONCLUSION

In recent years, significant progress has been made in cloud computing intrusion detection. The ever-growing cyber threat requires continuous improvement in security technology, especially in cloud computing environments. In this paper, we reviewed different intrusion detection techniques for cloud computing, including behavioral analysis, heuristic analysis, log analysis, correlation, and machine learning. The combination of AI and machine learning technologies has improved our ability to detect complex and sophisticated threats. While progress has been made, challenges remain, particularly in addressing security issues associated with cloud computing. New threats require continuous efforts for research and development. Therefore, it is necessary to enhance the security of cloud computing by integrating the techniques used in intrusion detection and adopting a collaborative approach to detect threats. In this paper, we presented the basis for research on threats and the methods and techniques used, which provides ideas for more flexible and efficient intrusion detection techniques

in cloud computing.

REFERENCES

[1] S. Dixit and G. Hussain, "An effective intrusion detection system in cloud computing environment," in *Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022,* (Springer, 2023), pp. 671–680.

[2] Geeta and S. Prakash, "Role of virtualization techniques in cloud computing environment," in *Advances in Computer Communication and Computational Sciences: Proceedings of IC4S 2017, Volume 2,* (Springer, 2019), pp. 439–450.

[3] S. Alam, M. Shuaib, and A. Samad, "A collaborative study of intrusion detection and prevention techniques in cloud computing," in *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1,* (Springer, 2019), pp. 231–240.

[4] P. Rana, I. Batra, A. Malik, *et al.*, "Intrusion detection systems in cloud computing paradigm: analysis and overview," Complexity **2022**, 3999039 (2022).

[5] S. Lata and D. Singh, "Intrusion detection system in cloud environment: Literature survey & future research directions," Int. J. Inf. Manag. Data Insights **2**, 100134 (2022).

[6] L. K. Vashishtha, A. P. Singh, and K. Chatterjee, "Hidm: A hybrid intrusion detection model for cloud based systems," Wirel. Pers. Commun. **128**, 2637–2666 (2023).

[7] S. Velliangiri, P. Karthikeyan, and V. Vinoth Kumar, "Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks," J. Exp. & Theor. Artif. Intell. **33**, 405–424 (2021).

[8] U. Islam, A. Al-Atawi, H. S. Alwageed, *et al.*, "Real-time detection schemes for memory dos (m-dos) attacks on cloud computing applications," IEEE Access (2023).

[9] N. Eddermoug, A. Mansour, M. Azmi, *et al.*, "A literature review on attacks prevention and profiling in cloud computing," Procedia Comput. Sci. **220**, 970–977 (2023).

[10] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, *et al.*, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Trans. on Emerg. Telecommun. Technol. **32**, e4150 (2021).

[11] J. L. Gutierrez-Garcia, E. Sanchez-DelaCruz, and M. d. P. Pozos-Parra, "A review of intrusion detection systems using machine learning: Attacks, algorithms and challenges," in *Future of Information and Communication Conference,* (Springer, 2023), pp. 59–78.

[12] N. TN and D. Pramod, "Insider intrusion detection techniques: A state-of-the-art review," J. Comput. Inf. Syst. **64**, 106–123 (2024).

[13] G. Luo, Z. Chen, and B. O. Mohammed, "A systematic literature review of intrusion detection systems in the cloud-based iot environments," Concurr. Comput. Pract. Exp. **34**, e6822 (2022).

[14] H. Asad, S. Adhikari, and I. Gashi, "A perspective–retrospective analysis of diversity in signature-based open-source network intrusion detection systems," Int. J. Inf. Secur. **23**, 1331–1346 (2024).

[15] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for iot application," Discov. Internet things **3**, 5 (2023).

[16] S. Alem, D. Espes, L. Nana, *et al.*, "A novel bi-anomaly-based intrusion detection system approach for industry 4.0," Future Gener. Comput. Syst. **145**, 267–283 (2023).

[17] A. Srivastava, "Swarm intelligence for network security: a new approach to user behavior analysis," Int. Res. J. Eng. Technol. **10**, 379–383 (2023).

[18] A. Kumar and T. K. Das, "Rule-based intrusion detection system using logical analysis of data," in *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT),* (IEEE, 2023), pp. 129–135.

[19] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, "Subject review: Intrusion detection system (ids) and intrusion prevention system (ips)," Glob. J. Eng. Technol. Adv. **14**, 155–158 (2023).

[20] A. Tedyyana, O. Ghazali, and O. W. Purbo, "A real-time hypertext transfer protocol intrusion detection system on web server," TELKOMNIKA (Telecommunication Comput. Electron. Control. **21**, 566–573 (2023).

[21] M. Çelebi, A. Özbilen, and U. Yavanoğlu, "A comprehensive survey on deep packet inspection for advanced network traffic analysis: issues and challenges," Niğde Ömer Halisdemir Univ. Mühendislik Bilimleri Dergisi **12**, 1–29 (2023).

[22] S. K. Shandilya, C. Ganguli, I. Izonin, and A. K. Nagar, "Cyber attack evaluation dataset for deep packet inspection and analysis," Data Brief **46**, 108771 (2023).

[23] Y. Zhang, M. Xue, H. Zhang, *et al.*, "Dual cuckoo filter with a low false positive rate for deep packet inspection," IEICE Trans. on Fundam. Electron. Commun. Comput. Sci. **106**, 1037–1042 (2023).

[24] A. Brown, M. Gupta, and M. Abdelsalam, "Automated machine learning for deep learning based malware detection," Comput. & Secur. **137**, 103582 (2024).

[25] Z. Sun, G. An, Y. Yang, and Y. Liu, "Optimized machine learning enabled intrusion detection 2 system for internet of medical things," Frankl. Open **6**, 100056 (2024).

[26] S. V. E. K. S. K. P. Elamparithi, S. Kalaivani and R. S. Raaj, "A machine learning approach for detecting ddos attack in iot network using random forest classifier," Int. J. Intell. Syst. Appl. Eng. **12**, 495–502 (2024).

[27] E. Osa, P. E. Orukpe, and U. Iruansi, "Design and implementation of a deep neural network approach for intrusion detection systems," e-Prime-Advances Electr. Eng. Electron. Energy **7**, 100434 (2024).

[28] J. Svacina, J. Raffety, C. Woodahl, *et al.*, "On vulnerability and security log analysis: A systematic literature review on recent trends," in *Proceedings of the International Conference on Research in Adaptive and Convergent Systems,* (2020), pp. 175–180.

[29] L. Liao, K. Zhu, J. Luo, and J. Cai, "Logbasa: Log anomaly detection based on system behavior analysis and global semantic awareness," Int. J. Intell. Syst. **2023**, 3777826 (2023).

[30] P. Ryciak, K. Wasielewska, and A. Janicki, "Anomaly detection in log files using selected natural language processing methods," Appl. Sci. **12**, 5089 (2022).

[31] M. Landauer, M. Wurzenberger, F. Skopik, *et al.*, "Aminer: A modular log data analysis pipeline for anomaly-based intrusion detection," Digit. Threat. Res. Pract. **4**, 1–16 (2023).

[32] M. Wurzenberger, G. Höld, M. Landauer, and F. Skopik, "Analysis of statistical properties of variables in log data for advanced anomaly detection in cyber security," Comput. & Secur. **137**, 103631 (2024).

[33] D. Jakhar and I. Kaur, "Artificial intelligence, machine learning and deep learning: definitions and differences," Clin. experimental dermatology **45**, 131–132 (2020).

[34] R. Kimanzi, P. Kimanga, D. Cherori, and P. K. Gikunda, "Deep learning algorithms used in intrusion detection systems–a review," arXiv preprint arXiv:2402.17020 (2024).

[35] N. Kaloudi and J. Li, "The ai-based cyber threat landscape: A survey," ACM Comput. Surv. (CSUR) **53**, 1–34 (2020).

[36] L. Sgaglione, L. Coppolino, S. D'Antonio, *et al.*, "Privacy preserving intrusion detection via homomorphic encryption," in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE),* (IEEE, 2019), pp. 321–326.

[37] S. Namasudra, "An improved attribute-based encryption technique towards the data security in cloud computing," Concurr. Comput. Pract. Exp. **31**, e4364 (2019).

[38] A.-R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, *et al.*, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," J. Cloud Comput. **12**, 127 (2023).

[39] V. Sarveshwaran, S. Pandiaraj, G. Bindu, *et al.*, "Binarized spiking neural network with blockchain based intrusion detection framework for enhancing privacy and security in cloud computing environment," Appl. Soft Comput. **154**, 111218 (2024).

[40] A. Padma and M. Ramaiah, "Blockchain based an efficient and secure privacy preserved framework for smart cities," IEEE

Access (2024).
[41] R. Kumar, P. Kumar, R. Tripathi, *et al.*, "A distributed intrusion detection system to detect ddos attacks in blockchain-enabled iot network," J. Parallel Distributed Comput. **164**, 55–68 (2022).
[42] Y. P. Tsang, C. H. Wu, and N. Dong, "A federated-anfis for collaborative intrusion detection in securing decentralized autonomous organizations," IEEE Trans. on Eng. Manag. (2023).
[43] Y. P. Tsang, C. H. Wu, and N. Dong, "A federated-anfis for collaborative intrusion detection in securing decentralized autonomous organizations," IEEE Trans. on Eng. Manag. (2023).
[44] B. Sharma, P. Pokharel, and B. Joshi, "User behavior analytics for anomaly detection using lstm autoencoder-insider threat detection," in *Proceedings of the 11th international conference on advances in information technology,* (2020), pp. 1–9.
[45] S. O. Olabanji, Y. Marquis, C. S. Adigwe, *et al.*, "Ai-driven cloud security: Examining the impact of user behavior analysis on threat detection," Asian J. Res. Comput. Sci. **17**, 57–74 (2024).
[46] T. Theodoropoulos, L. Rosa, C. Benzaid, *et al.*, "Security in cloud-native services: A survey," J. Cybersecur. Priv. **3**, 758–793 (2023).
[47] P. Surace, "Anomaly detection in cloud-native systems," Master's thesis (2019).
[48] M. Müller, D. Behnke, P.-B. Bök, *et al.*, "Cloud-native threat detection and containment for smart manufacturing," in *2020 6th IEEE Conference on Network Softwarization (NetSoft),* (IEEE, 2020), pp. 347–349.