iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** VI **Month of publication:** June 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.83605

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

# Enhancing Security in Serverless Cloud Computing Using AI-Based Intrusion and Anomaly Detection: A Comprehensive Review

Mr. Aditya Bhogale, Dr. Suhas Rautmare
*Dept. of Information Technology, University of Mumbai, Mumbai, India*

***Abstract:*** ***Serverless computing has become popular for cloud computing mainly because it makes scaling easier, costs less, and calls for less managing of infrastructures. These days though there are a lot of security issues with serverless that limit its broader adoption. And usually, traditional security methods don't really work well with serverless architectures, given their dynamic and distributed nature. Because of this, the need for intelligent systems, which can not only detect but also identify sophisticated cyber threats hidden through intrusion and anomaly detection, is rising. AI and ML are the latest technologies holding potential for improving security at serverless cloud environments Mostly in threat detection and behavioral analysis. This study analyzes 40 research articles from 2020 to 2026, among them are serverless security, intrusion detection systems based on cloud, anomaly detection techniques, machine learning and deep learning methods, Explainable Artificial Intelligence (XAI), federated learning, adversarial machine learning, cloud-native security setups, and self-supervised learning. As the literature that has been examined, behavioral pattern analysis in cloud telemetry, execution logs, and network traffic allows AI-driven techniques to effectively detect attacks. Besides, advanced AI-based methods such as deep learning, self-supervised learning, federated learning, and explainable AI do drastically enhance detection accuracy scalability adaptability, and trustworthiness in serverless cloud systems. The review has also pointed out some research problems that have not been solved so far, including the shortage of labeled datasets, the requirement for large-scale real-time monitoring, the ability to be fooled by adversarial attacks, concerns about model interpretability, and privacy issues. At the end of the paper, research gaps are identified as well as future theoretical development directions for secure, intelligent, and resilient serverless cloud computing environments.***

## I. INTRODUCTION

### *A. Cloud Computing*

Cloud computing is a means of accessing a pool of computing resources over the internet. It offers tremendous flexibility and efficiency for businesses. It reduces their costs. It allows scalability. There are three most common types of service models. Infrastructure as a Service gives virtual machines to run applications and store data. Platform as a Service gives a platform to develop applications. Software as a Service deploys pre-developed applications. Businesses do not need to buy costly hardware and can run multiple applications remotely. All healthcare, finance, education, and e-commerce have digitally migrated their operations with the help of cloud evolution. Many questions remain about how these parts of the digital revolution happen continuously. But growth presents issues. Data security is more important than ever. There are increasing numbers of security threats. Managing resources is more difficult. Security issues become a concern as its use grows.

### *B. Serverless Computing*

Serverless computing is a new model in cloud computing that offers an unprecedented level of ease and simplicity for developers, because they no longer have to worry about managing servers or the underlying infrastructure. Essentially, in a serverless setup, the cloud provider takes care of all the resource provisioning, scaling, maintenance, and availability aspects, so developers only need to work on the application logic. Using Function-as-a-Service (FaaS) platforms such as AWS Lambda, Azure Functions, and Google Cloud Functions has not only made the process of application deployment very easy but has also significantly cut down the operations cost. Serverless-based systems can be used to develop event-driven applications, microservices, and cloud-native systems; this way, they are very well aligned with highly dynamic and scalable workloads. Still, the hiding of the infrastructure layer that comes with serverless computing does create certain security issues that necessitate a level of protection that is more sophisticated.

### C. Security Challenges in Serverless Computing

The highly dynamic and distributed architecture of serverless computing leads to a very different security environment. Compared to traditional cloud settings, serverless functions are ephemeral, rely on events, and can scale extremely well, which poses greater difficulties to continuous monitoring and threat detection. Security risks encompass function hacking, vulnerable third-party libraries, privilege escalation, illegitimate access, data exposure, misconfigurations, and denial-of-wallet attacks. What's more, the shared nature of multi-tenant cloud environments make it easier for resource abuse and cross-function attacks to happen. Besides, the quick lifecycle of functions also undermines the potential of standard security measures, which results in the inability to detect complex threats swiftly. With the growing use of serverless platforms by organizations for their most important applications, finding solutions to these security issues has become a key research area.

### D. Need for AI-Based Intrusion and Anomaly Detection

Traditional security methods and signature-based Intrusion Detection Systems (IDS) usually fail to catch the latest cyber threats in serverless environments. Sophisticated attacks often take advantage of undisclosed vulnerabilities and produce behavioral traits that no signature can recognize. AI, ML, and DL are effective tools that can equip security systems with the ability to understand intricate patterns derived from massive cloud data and automatically pinpoint deviations. With AI, intrusion and anomaly detection systems get better at boosting detection accuracy, lowering false alarms, and responding to new attack methods. Self-supervised learning, federated learning XAI adversarial machine learning, and cloud-native security structures are a few of the recent innovations that have Much improved the power of smart security systems. These advances are vital in safeguarding serverless environments against all types of cyber threats - those that are known and those that are not.

### E. Research Objectives

The research aim to explore state-of-the-art AI techniques for intrusion and anomaly detection in our review paper as a major means for enhancing serverless cloud security. Besides analyzing current detection schemes and identifying the loopholes of recent literature, this paper also wishes to cover the aspects of how cloud-native security setups, observability tools, explainable AI, federated learning as well as anomaly detection models can be integrated to bolster the resilience and security of serverless computing environments.

### F. Contributions of the Paper

The major contributions of this review paper are summarized as follows:

1) A detailed study of the latest papers on serverless computing security, cloud security, intrusion detection systems, and anomalous behavior detection methods.
2) Study of Artificial Intelligence, Machine Learning, Deep Learning, Self-Supervised Learning, Federated Learning, and Explainable AI methods applied to identify security threats.
3) A contrast on the existing cloud-native security structures and serverless security mechanisms.
4) Listing of prime security threats, vulnerabilities, and challenges in serverless cloud environments.
5) Review of developing technologies like Zero Trust Architecture, Intelligent Security Service Setups, Observability-based Security Assessment, and AI-driven anomaly detection models.
6) Outlining potential areas of research and future trends for intelligent, scalable, and resilient serverless cloud computing security solutions.

## II. BACKGROUND

### A. Serverless Computing Fundamentals

Serverless computing is essentially an updated version of cloud computing. Not only does it enable the developers to write and execute an app without worrying about the server, but the cloud service providers also take over the entire server task from them. The cloud team will do things like resource allocation, scaling, and management, so software developers will have only one task - to write the application's main features. Mainly, FaaS or Function as a Service is a serverless model component. It breaks down an application into multiple smaller functions that execute in response to different events. This can help make the usage of resources more efficient as a function is executed only when the corresponding event takes place.

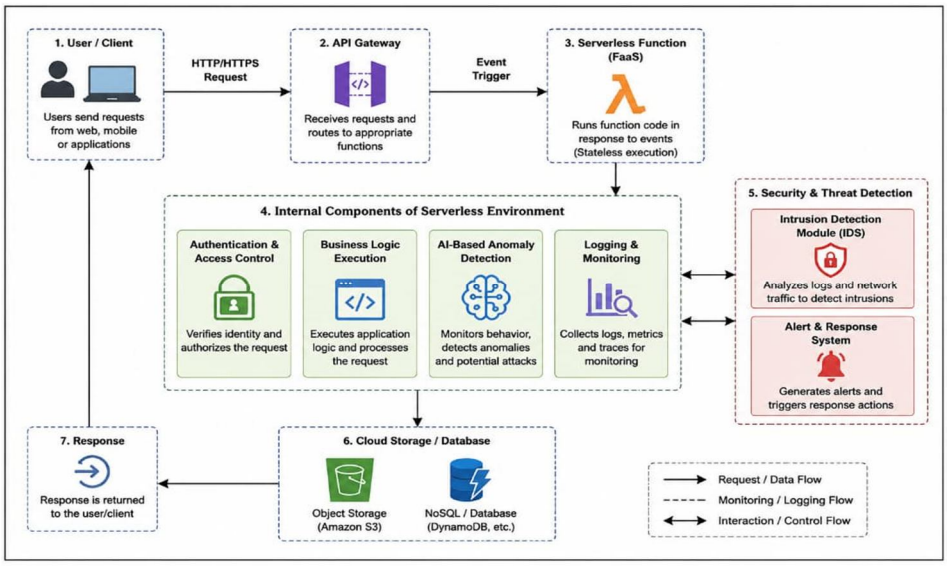



Fig. 1. Architecture and workflow of a serverless computing environment with AI-based intrusion and anomaly detection

Figure 1 shows the fundamental structure of a serverless computing environment. User requests are directed via an API Gateway to serverless functions. At these serverless function points authentication monitoring, intrusion detection, and AI-based anomaly detection systems work in conjunction before the cloud storage services are accessed and the responses are generated.

Leading platforms for serverless are AWS Lambda, Microsoft Azure Functions, and Google Cloud Functions. Resource allocation is transformed into a dynamic activity with the help of both instant and automatic scaling. The serverless model is nowadays extensively utilized in cloud-native apps microservices web services, and the Internet of Things (IoT). Aside from creating more opportunities for the constant efficient and affordable scaling of the enterprises, one of the main advantages of serverless cloud computing is billing on the pay-per-use basis. In this way, the businesses can save money by this.

However, server-less computing has some drawbacks as well. Amongst others, limitations in visibility, cold start times, managing dependencies, and vendor lock-in, might negatively affect both application development and management. Security risks are also brought about by the very nature of serverless environments. So, new advanced techniques are needed to spot security threats in the serverless cloud computing environment.

### *B. Security Challenges in Serverless Environments*

Serverless computing brings with it a different set of challenges related to security as its inherently dynamic and distributed nature. The short-lived functions of serverless applications are different in that they respond to events and can run on a shared cloud infrastructure, which is unlike the cloud systems that people are traditionally used to. This new system architecture complicates tasks like monitoring, access control, and threat detection. A big issue is the little insight you have into the execution environment. On top of not having control over the management of the infrastructure, organizations don't even have much access to system-level logs and runtime information because it is the cloud providers who handle it. This is likely going to be a big roadblock to incident investigation and security auditing. Also, serverless applications are highly dependent on third-party libraries and external services, which are potential sources of vulnerabilities due to insecure dependencies.

Data security is an equally important issue. Secret information handled by serverless functions can get leaked in many ways like using wrongly set permissions, insecure APIs, or the wrong storage methods. Hackers may also manipulate function triggers, take advantages of privilege escalation weaknesses and authentication errors to get access to cloud resources without permission. Besides, the shared characteristic of cloud environments multiplies risks like multi-tenancy and resource abuse.

Among the threats specific to serverless computing, there is one called denial-of-wallet attack where the attacker keeps on triggering the cloud function so that the cost of operation becomes high, so hurting the victim. To make things even more challenging, functions can be created and terminated very quickly; all these factors together render conventional security measures less effective. As a result, the infrastructures of serverless must be protected with new enhanced monitoring, intrusion detection, and anomaly detection techniques.

### C. Intrusion Detection Systems

Intrusion Detection Systems (IDS) are a type of security tool that, among other things, keep an eye on network traffic, system activities and applications behavior to identify any malicious actions or violations of rules. IDS systems are very important in the area of cloud computing security. These systems can monitor constantly and at the same time detect cyber threats early and so prevent any damage to confidentiality, integrity and availability of the data. Generally, IDS approaches are divided into three categories signature-based, anomaly based and hybrid systems. Signature-based IDS detects known attacks by comparing activities against stored attack patterns. Even though this approach is very effective in dealing with known threats, these systems still have limitations when it comes to identifying new attacks. Anomaly-based IDS addresses this issue by first establishing a model of normal behavior and then detecting deviations that could indicate malicious activity. Hybrid IDS combines both approaches to improve detection rate and reduce false alarms.

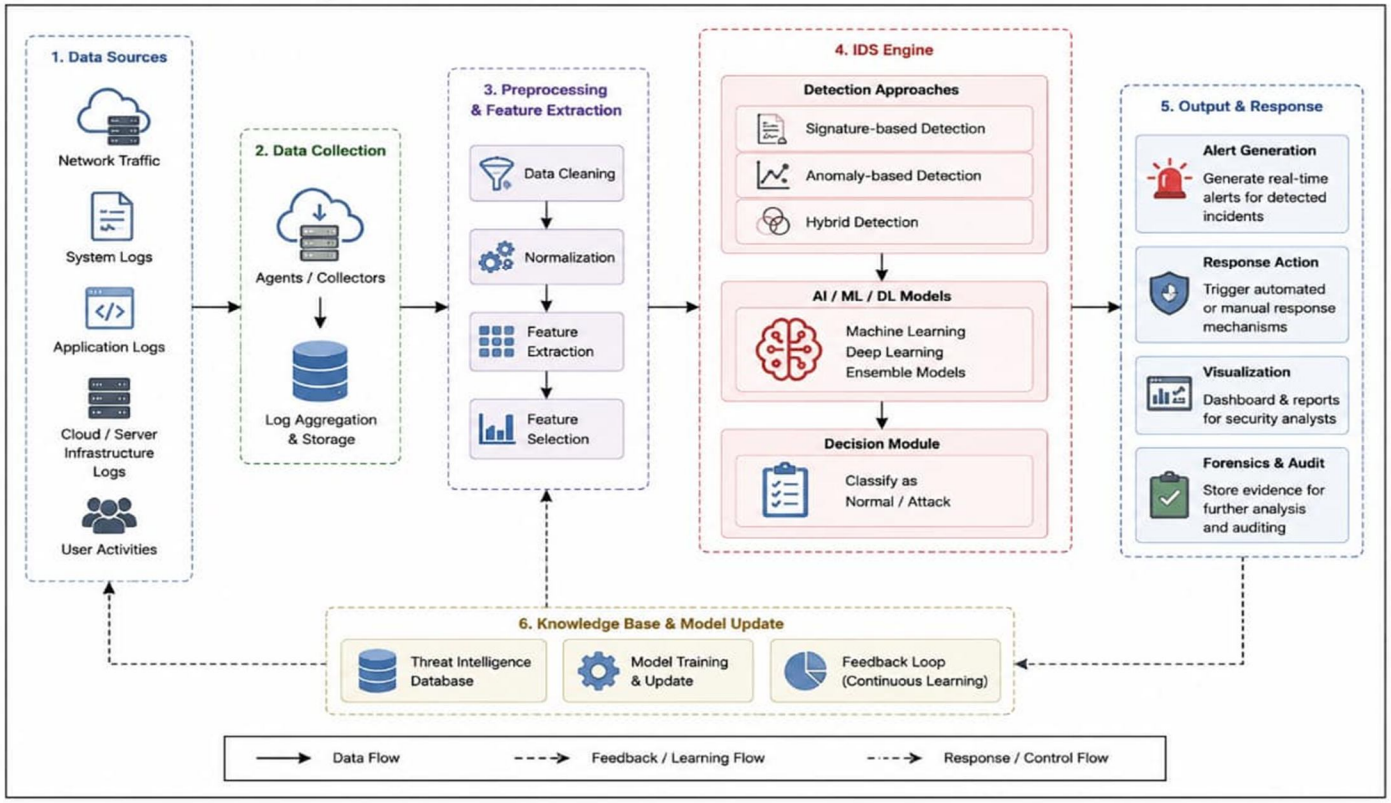



Fig. 2. AI-based intrusion detection system architecture

Figure 2 shows how an AI-assisted Intrusion Detection System (IDS) works. The process starts with collecting data from places such as network traffic, system logs, application logs, cloud infrastructure logs and user activities. This data is then prepared and transformed into features for the IDS engine to analyze. The IDS uses detection methods like signature-based or anomaly-based detection or a mix of both. It also uses machine learning and deep learning techniques to detect harmful activities. When a breach happens the IDS sends out warnings. Takes necessary actions. The IDS also learns from its experiences. Updates its models to fight new types of cyber-attacks. The IDS engine relies on the data, detection methods and machine learning to identify threats.

The overall flow of work helps the IDS to improve its detection and response, to cyber-attacks. In a cloud environment IDS may be implemented in the form of Host-Based Intrusion Detection Systems (HIDS) or Network-Based Intrusion Detection Systems (NIDS). HIDS is mainly concerned with monitoring the activities of the individual systems whereas NIDS is focused on the network traffic within the cloud infrastructures. Machine learning based IDS systems will be the mainstay of the modern cloudy environment, as ML brings increased and faster adaptability to threats. IDS, although very beneficial, have to deal with problems like high false positive rates, limited ability to scale, difficulties in analyzing encrypted traffic and lack of sufficient power to deal with sophisticated attacks. The growing popularity of cloud-native and serverless computing has motivated investigators to adopt artificial intelligence and machine learning for enhancing detection systems.

*D. AI-Based Anomaly Detection*

Nowadays, the role of Artificial Intelligence in cybersecurity is substantial, as it can analyze huge volumes of data and detect attack patterns that might be overlooked by human analysts. Cloud and serverless platforms, in particular, are increasingly leveraging artificial intelligence in an effort to identify suspicious behavior that traditional security methods could miss.

Artificial Intelligence systems analyze data patterns to determine whether a certain event or entity is normal or suspicious. These detection methods can be broadly classified into three types according to the amount of labeled data available for training: supervised, unsupervised and semi-supervised.

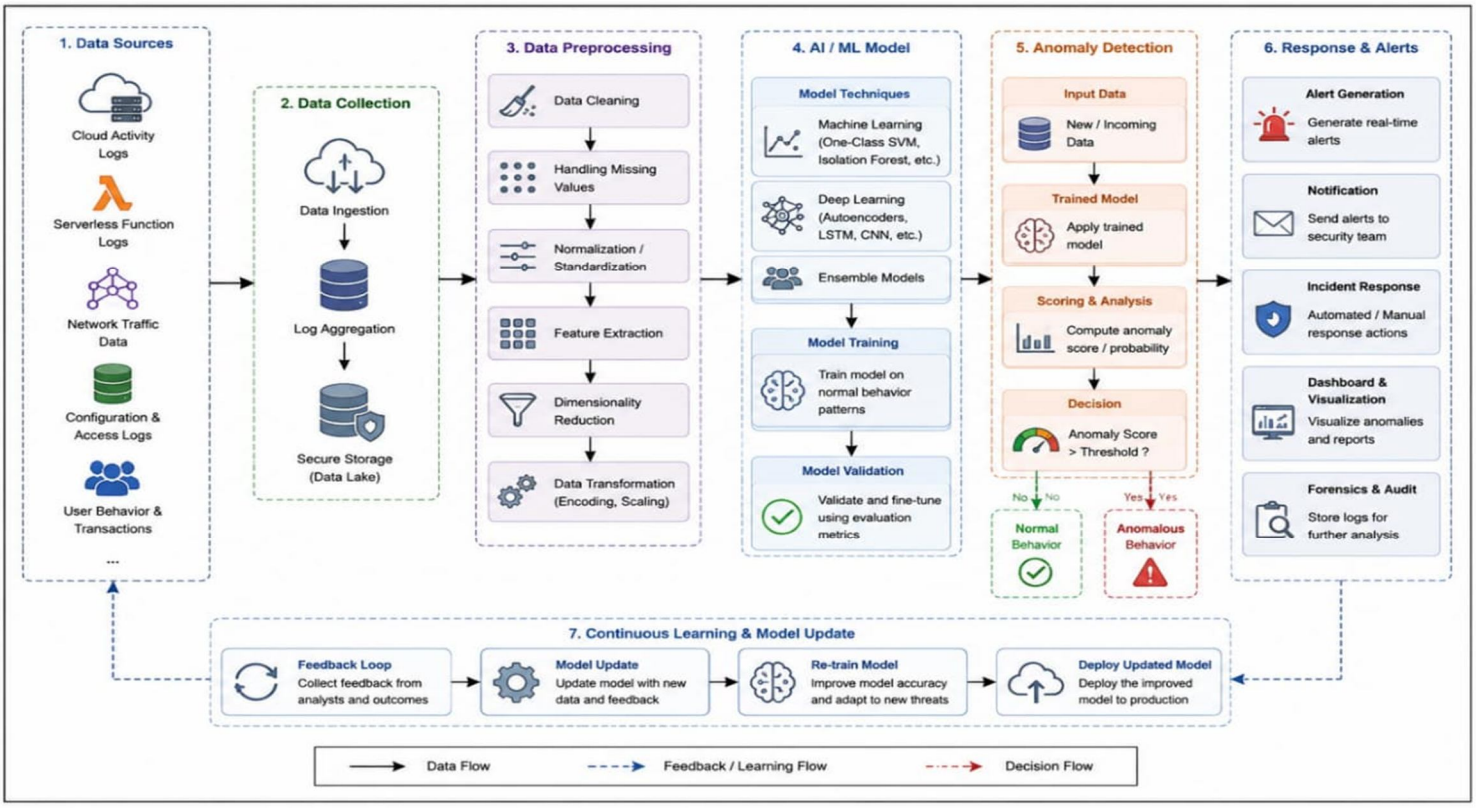



Fig. 3. Workflow of AI-based anomaly detection in cloud computing

Figure 3 shows how AI finds activities in cloud environments. We get data from places such as logs of what happens in the cloud, logs of serverless functions, network traffic, and what users do. After we clean up the data and figure out what is important, we use machine learning and deep learning to look at how things work. This helps us find activities and send out warnings. The systems keep learning all the time, so they get better at finding activities by looking at new threats and how the systems change over time. Driven anomaly detection in cloud environments is what makes this work. Certain types of models, such as deep-learning ones, are very efficient at detecting attacks by extracting salient features from large datasets.

AI-driven security tools have the capability to continuously monitor workload executions, network traffic, user activities and serverless function operations simultaneously. Besides that, they are extremely effective in detecting attacks, identifying insider threats, and uncovering unusual resource usage, and they outperform conventional security solutions in this way. Alongside the emergence of self-supervised learning, federated learning and explainable AI together are transforming these security capabilities, making them stronger, larger, and more transparent.

There are advantages to using AI-based security techniques, as well as some significant drawbacks that should be kept in mind. Issues such as models' explainability, data privacy, susceptibility to adversarial attacks, and scaling costs might interfere with system performance. Despite all these challenges, for intrusion detection and anomaly identification in cloud and serverless computing, AI remains one of the best options. It is very significant, mainly for cloud and serverless computing, and at the same time it is constantly evolving in its crime-discovery ability.

## III. CLASSIFICATION OF EXISTING RESEARCH IN SERVERLESS CLOUD SECURITY

The fast move to serverless computing has brought security issues that need better protection than what we have now. People are looking into ways to solve this problem. They are thinking about things like finding intruders and catching activities and using artificial intelligence to make security systems. They are also looking at ways to protect serverless systems. All these studies are different because they are looking at things and using different methods. So, it is an idea to put all these studies into groups that make sense. We can put these studies into five groups: the security problems of serverless systems finding intruders, in the cloud using artificial intelligence to catch strange activities systems that are made just for serverless and new security systems. This helps us see how research is changing and find the ideas, strong points and areas that need more work to make serverless cloud security better. Serverless computing is a deal and serverless security is very important. Serverless security is what we need to focus on to make serverless computing safe.

### *A. Serverless Security Challenges*

Several researchers have looked into the security risks that come with serverless computing environments. Ahmadi [1] discussed the main network security challenges in serverless platforms and suggested ways to secure cloud-native services. Marin et al. [7] offered a detailed view of security in serverless computing and pointed out vulnerabilities tied to function isolation, event triggering, and resource sharing. Dorsett et al. [8] reviewed denial-of-wallet attacks and showed how attackers take advantage of automatic resource scaling to raise operational costs. Li et al. [20] investigated security challenges, available countermeasures, and future chances for securing serverless architectures. Similarly, Janumpally [21] looked at privacy and data protection issues in serverless environments. Ni et al. [25] introduced ways to measure security risks in serverless platforms. Escaleira et al. [27] summarized the current security mechanisms and identified research gaps that need further exploration.

### *B. Cloud Intrusion Detection Systems*

Research on cloud intrusion detection systems has concentrated on improving attack detection accuracy and reducing response time. Mahendar and Shivakanth [2] examined machine learning-based IDS approaches for cloud security and pointed out their benefits over traditional detection methods. Othman et al. [3] looked at various intrusion detection mechanisms used in cloud environments and compared their effectiveness. Al-Ghuwairi et al. [5] suggested a machine learning-based anomaly detection method using time-series analysis for cloud security monitoring. Lata and Singh [22] reviewed existing IDS architectures and talked about future research directions. Xu et al. [10] provided a thorough survey of deep learning-based IDS techniques and showed the growing use of neural-network-based detection models.

### *C. AI-Based Anomaly Detection*

Artificial Intelligence has become one of the most commonly used methods for detecting anomalies in cloud environments. Darban et al. [12] reviewed deep learning techniques for time-series anomaly detection and looked at how they can be used in different fields. Whitman et al. [16] studied machine learning techniques for anomaly detection in serverless cloud environments. Islam et al. [17] provided a dataset for industry-scale cloud anomaly detection and showed the challenges in practical deployment. Zhong et al. [23] examined anomaly detection methods used in AIOps systems and pointed out new trends in operational intelligence. Paparrizos et al. [29] reviewed modern anomaly detection algorithms, benchmarks, and evaluation methods. Recently, Li et al. [40] introduced SAFE, a self-supervised anomaly detection framework that can identify previously unseen attacks without needing labeled training data.

### *D. Serverless-Specific Detection Systems*

Several research works proposed security solutions for serverless environments. Nguyen et al. [6] studied silent failures in stateless systems and put forward that anomaly detection methods in serverless applications need to be improved. Lavi et al. [9] proposed methods for locating compromised functions in serverless cloud infrastructures. Li et al. [18] presented FaaSMT, a lightweight intrusion detection setup that merges Merkle Trees with task inlining techniques to enhance security. Jegan et al. [19] brought SecLambda, a structure to secure serverless applications through runtime monitoring and policy enforcement. Yan et al. [26] came up with the Intelligent Security Service Setup (ISSF), through which AI security services are integrated into cloud-native environments. Shin et al. [36] came up with Bambda, a real-time verification system for monitoring and validating serverless function execution.

### *E. Emerging Security Approaches*

Recent research has looked into new technologies to overcome the limitations of traditional intrusion detection systems. D'Almeida e Mendes and Rios [30] studied how Explainable Artificial Intelligence (XAI) can be used in cybersecurity. Rjoub et al. [31] examined explainable AI techniques and how they can help build trust in security systems. Khraisat et al. [32] and Agrawal et al. [33] investigated intrusion detection methods based on federated learning, which allows for collaborative model training while keeping data private. Alhajjar et al. [34] highlighted threats from adversarial machine learning to intrusion detection systems, while Ennaji et al. [35] reviewed recent adversarial challenges and future research paths. Borges et al. [37] introduced security assessment methods based on observability for cloud-native systems. Dkmak et al. [38] proposed an AI-driven algorithm for detecting anomalies in microservices. Arora and Hastings [39] showed the security advantages of microsegmentation and Zero Trust architectures in cloud-native environments.

## IV. LITERATURE REVIEW

The literature on serverless cloud security has grown a lot in recent years. This is due to the increasing use of Function-as-a-Service (FaaS) platforms and cloud-native architectures. Researchers have suggested different ways to tackle security challenges. These include intrusion detection systems, anomaly detection techniques, machine learning models, and security frameworks. Existing studies aim to improve threat detection accuracy, cut down response time, and boost the overall security of serverless environments. To give a clear view of current developments, the reviewed literature is divided into five main areas: serverless security challenges, cloud intrusion detection systems, AI and machine learning-based anomaly detection, anomaly detection in serverless environments, and new security models.

### *A. Serverless Security Challenges*

Serverless computing's extensive adoption has completely transformed the deployment and management of cloud applications by automating scaling, reducing operational overhead, and enhancing resource utilization. Yet, serverless setups bring up a different set of security issues from those of traditional cloud architectures. For example, the management of infrastructure is completely hidden, the execution is based on events, and a great deal of third-party services are used, all of which lead to new threats that require security measures of a different kind.

A number of scholars have gone into detail about the risks tied to serverless computing. For example, Ahmadi [1] pointed out the most critical issues, such as unauthorized access, insecure data transmission, dependency vulnerabilities, and poorly implemented monitoring mechanisms. It was also revealed that serverless platforms, while making it easy to deploy applications, have their downside in that they reduce the visibility of the underlying infrastructure, so making security more difficult.

In brief, Marin et al. [7] also presented a detailed security examination of serverless computing that includes various threats related to the insecure execution of functions, manipulation of event data, and privilege-escalation attacks. This research shows that traditional security tools do not suffice when it comes to the protection of very dynamic serverless workloads.

Recently, Li et al. [20] have drawn attention to the security risks and the areas of serverless computing that need to be protected, including how the security of a serverless function can be compromised in different ways: through third-party libraries or services, various types of dependency issues, malicious packages, insecure APIs, or access permissions that are not properly configured. Janumpally [21] has taken up the topic of data in serverless environments, and in particular data privacy and confidentiality, which are the main points that he mentioned can also be threatened, leading to a data leak through the misconfiguration of data isolation mechanisms. Economic and operational attacks in serverless environments have been considered by Dorsett et al. [8], who have demonstrated Denial-of-Wallet attacks, a very dangerous scenario in a serverless computing environment where the attackers can perform a DOW attack by sending overflow amounts of requests for invocations of the serverless functions, driving up the function invocations and eventually exhausting the budget of the serverless service provider. In addition, some very specific security challenges of serverless computing related to particular industries have become a great concern, leading to research papers. Kumar [24], for example, showed the security challenges of serverless computing in the healthcare industry, where serverless security challenges arise from collecting sensitive information, limited security capabilities of IoT devices, and the need to meet regulatory compliance. Ni et al. [25] have suggested ways to quantify serverless security so that organizations can assess and measure the security risks associated with the use of serverless computing platforms. As serverless applications have come to represent the majority, some researchers have been motivated to look at the security components and identify the security issues of serverless computing. Escaleira et al. [27] put forth a systematic review of serverless security mechanisms, and in their findings they mentioned that there are limitations even in the existing solutions for authentication, authorization, and runtime protection.

Pathade et al. [28] reported that combining machine learning tasks in serverless settings introduces risks including model poisoning, adversarial manipulations, and inference attacks. Besides cloud-related issues, the review of related literature points out several security challenges in serverless computing. These challenges are less visibility, dependency, economic attacks, privacy, as well as AI-specific threats that call for better detection of intrusion and anomaly in serverless computing.

### *B. Intrusion Detection Systems in Cloud Computing*

Cloud computing has attracted huge attention from researchers and service providers due to its unique features and huge potential in providing computing resources and services. However, it is evident that the cloud environment is not an isolated system that is not immune to cyberattacks. Given the latent threat to cloud computing security, intrusion detection systems (IDS) have emerged to play a crucial role in detecting security incidents, attacks and policy violations before they inflect damage and loss of assets to cloud systems. The IDS purpose of detecting and identifying both conventional and novel attacks and security violations that cannot be effectively addressed by traditional security techniques such as firewalls and access control systems, hence the need to integrate IDS with cloud security. In this section, a systematic survey on machine learning and other IDS techniques is reviewed in terms of their recent developments, necessities, and various challenges facing in cloud computing security. Mahendar and Shivakanth [2] have highlighted the importance of intelligence learning algorithms in enhancing the detection ability of IDS. Whereas, Othman et al. [3] have surveyed various IDS techniques in cloud computing and argued the significance of anomaly-based IDS in detecting evolving cyberthreats.

Al-Ghuwairi et al. [5] introduced an intrusion detection framework for cloud systems based on time-series anomaly analysis and machine learning techniques. The designed framework has shown to be an effective intrusion detection technique by analyzing the behavioural patterns; thus, it outperforms the conventional IDS.

Hence, deep learning seems to be another technology as a defense against cloud intrusion. Xu et al. [10] discussed the strengths of deep learning models for feature extraction and attack classification. Also, they dealt with deep learning based IDS approaches and the merits of attracting neural network on feature extraction and attack detection. The authors concluded that neural network could be applied for the initial stage of attack detection and would be affordable within cloud when the huge dataset is not available with the cloud. However, the authors also had some concerns on the heavy computational power, interpretation of attack, and high training data. In recent work, researchers have tried to develop hybrid methods of attacks on cloud environments. Alhusseini et al. [11] proposed a hybrid framework of IDS which is based on AI and meta-heuristic optimization. They have reported that their proposed approach is able to achieve high accuracy and minimize the false alarms compared to prior IDS models.

Al-Husseini [13] also published a proposed hybrid IDS architecture which can be considered in the light of adaptability regarding cloud attacks. On the other hand, Lata and Singh [22] reviewed the importance of cloud intrusion detection system. They mentioned steps that would be required to reach the adaptable and smarter IDS as well as their challenges and the requirements of IDS to be adapted to cloud environments. In conclusion, the paper sheds light on the significant change that cloud intrusion detection system experience from the initial signature-based system to AI-based systems. These systems have been revolutionized by machine learning and deep learning which imparted a remarkable transformation in the cloud intrusion detection technology. Although numerous hindrances such as false positive alerts, scalability, and interpretability have still been a topic of debate in many studies.

### *C. AI and Machine Learning-Based Anomaly Detection*

Artificial Intelligence (AI) and Machine Learning (ML) technologies offer new and strong ways to detect anomalies and spot cyber threats within cloud computing environments. Unlike traditional rule-based systems, AI-driven approaches gain insights by training on huge sets of data and learning complex behavioral patterns. They can also automatically detect deviations which are potential indicators of a malicious activity. As cloud environments become more dynamic and distributed, anomaly detection is becoming a necessary element of contemporary cybersecurity structures.

Darban et al. [12] made a survey of deep learning techniques for time-series anomaly detection and also described how these methods are very effective in the analysis of sequential data produced by cloud systems. They found that deep learning programs are able to model complex temporal relationships and pick up on minor changes in behavior that are related to cyberattacks. This ability makes deep learning very well geared to keeping track of cloud workloads and uncovering unknown threats. The use of machine learning for anomaly detection has recently been expanded even to serverless cloud environments.

Whitman et al. [16] studied machine learning techniques for finding abnormal behavior in serverless applications and showed that smart models can spot suspicious execution patterns with a much better accuracy compared to traditional monitoring techniques. Their research implies that machine learning may be quite valuable in safeguarding agile Function-as-a-Service (FaaS) platforms.

Due to the scarcity of realistic datasets, the data availability issue remains as one of the biggest constraints in anomaly detection research. Islam et al. [17] presented a large-scale industry dataset for cloud anomaly detection and illustrated the practical problems facing the implementation of detection systems in real-world scenarios. Their research pointed out how vital it is to have representative datasets to assess detection performance and enhance model reliability. Operational intelligence is another major topic in current pieces of research. Zhong et al. [23] made an overview of the anomaly detection techniques in the AIOps area and stressed the importance of artificial intelligence in automating cloud operations and incident management. The research paper documented that AI-powered monitoring systems are capable of not only raising the level of operational efficiency but also lowering the workload of security analysts. At the moment, the focus is on enhancing anomaly detection with greater accuracy and lower dependence on labeled data. Paparrizos et al. [29] carried out a study on the latest productions of time-series anomaly detection algorithms and came up with benchmark evaluation techniques for contrasting detection results. Dkmak et al. [38] offered the Night's Watch Algorithm, an AI-powered anomaly detection system that targets cloud-native microservices. As their tests, their method led to better detection results in the settings of highly distributed applications. Li et al. [40] came up with SAFE, a novel self-supervised anomaly detection system that is capable of drawing out effective representations without the need for large amounts of labeled data. This method goes after a major drawback of the old-school machine learning systems and enhances the detection of new kinds of attacks. Taken all together, these works illustrate that AI and ML have pushed forward the state-of-the-art in anomaly detection in cloud computing by quite a margin. Still, problems like interpretability, computational complexity, adversarial robustness, and data quality will keep the researchers busy and lead to new research directions.

### *D. Anomaly Detection in Serverless Environments*

The distinct features of serverless computing impose difficulties on conventional anomaly detection solutions. Serverless applications are built out of ephemeral functions executing on demand that dynamically respond to events. This imposes constraints on runtime observability, at the same time as workloads are highly variable over short periods of time. The former demands anomaly detection techniques that can track very dynamic environments, minimizing overhead impacts.

Nguyen et al. [6] investigated silent failures and anomalies in a stateless system. They observed that traditional anomaly detection techniques commonly encounter failures in serverless environments. Their work demonstrated that lack of persistent system states makes it difficult to identify behavioral baselines for anomaly detection. They emphasized the importance of context-aware anomaly detection approaches at the functional level. Recent work also points out that discovering compromises is important in serverless security research. Lavi et al. [9] proposed a setup for detecting a compromised serverless function by behavioral profiling and anomaly detection. They demonstrated that profiling execution behaviors can detect both malicious modifications and unauthorised activities of cloud functions. Further, there have been efforts to discover lightweight security solutions for resource-constrained serverless environments. For example, Li et al. [18] built FaaSMT, a lightweight intrusion detection system utilizing a hybrid Merkle Tree verification and task inlining method. This system enhances security detection and leverages fewer computational resources, which is practical in large-scale serverless systems. Runtime security solutions have been explored as well. Jegan et al. [19] introduced a security architecture called SecLambda which protects serverless applications from runtime attacks. This security architecture tracks function execution at runtime and limits access per the set security policies.

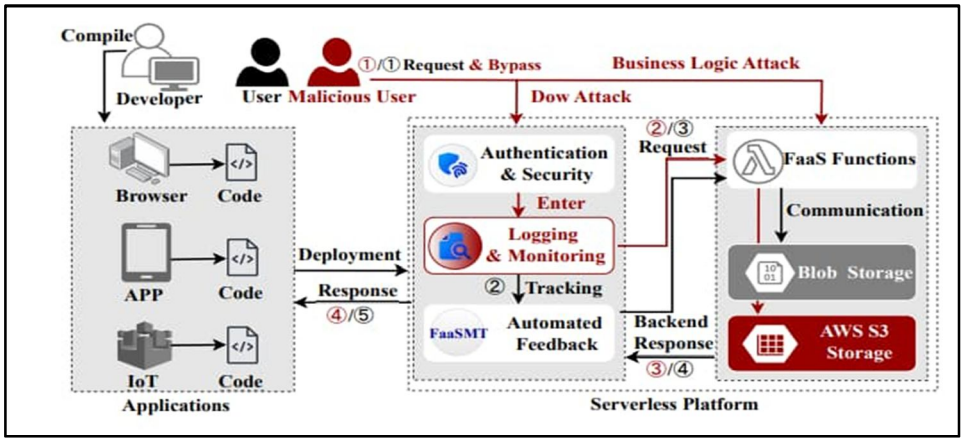



Fig. 4. Serverless architecture interaction process and deployment workflow of the FaaSMT framework (Adapted from Li et al. [18])

Results demonstrated that increasing security controls in serverless execution contexts can quite a bit help intrusion detection. A more recent example is from Shin et al. [36] who introduced Bambda. This is a setup for real-time verification in serverless computing that continuously checks the behavior of function execution to identify anomalies, signifying potential security breaches or failures. Their work highlights the need for such real-time validation.

In general, the papers point to the need for a tailor-made anomaly detection system in serverless computing, which takes into account evolution of execution patterns, reduced visibility, and resource limitations. The papers summarized above have demonstrated how much improvement has been made in applying anomaly detection techniques to the serverless system when discussing security.

### *E. Emerging Security Paradigms*

The fast-changing nature of cloud computing and cyber threats has led researchers to look for security techniques beyond conventional intrusion detection and anomaly detection methods. Recently, Explainable Artificial Intelligence (XAI), Federated Learning, Adversarial Machine Learning, Cloud Observability, and Zero Trust Architecture have become more and more integrated into the cybersecurity structures of the digital age. These technologies focus on bringing about greater transparency privacy reliability, and adaptability.

Yan et al. [26] came up with the Intelligent Security Service Structure (ISSF) that leverages reinforcement learning to enable cloud-centric security operations. This system not only adjusts to the changing setting but also demonstrates how intelligent decision-making models are increasingly taking up the cybersecurity role. Such techniques pave the way for automatic threat counteractions and continuous security evolutions in the cloud environment. The surge in machine learning application in security areas has made Explainable Artificial Intelligence a really vital research field.

Mendes and Rios.[30] carried out a systematic review of XAI in cybersecurity and pinpointed the requirement for security decisions to be transparent and understandable. Same thing, Rjoub et al. [31] explored explainable AI methods and highlighted how they can be used to nurture trust in AI-based intrusion detection through the provision of a comprehensible rationale of model's forecasting. Learning that preserves privacy is another significant component of research.

Khraisat et al. [32] and Agrawal et al. [33] investigated Federated Learning-based intrusion detection systems. These allow participants to collectively train the model while keeping their data private. Addressing privacy concerns, they at the same time ensure robust threat detection in distributed environments.

Another aspect of using AI for security-related purposes that has gained attention lately is the robustness of these solutions. Alhajjar et al. [34] examined adversarial machine learning tactics targeting intrusion detection systems and revealed how attackers could manipulate model inputs to stay undetected. Ennaji et al. [35] took a step further to analyze adversarial challenges and propose possible defense mechanisms to enhance the model's immunity against sophisticated attacks. Cloud observability and Zero Trust architectures are two more aspects that contribute to the enhancement of cloud security.

Borges et al. [37] came up with OXN, which is a system for automated vulnerability assessment that increases the visibility of cloud-native applications and enables proactive threat discovery. Dkmak et al. [38] adopted an AI-based method for anomaly detection within microservices ecosystems, which not only reaffirms the security in a cloud setting but also exemplifies how these kind of services can matter a lot in threat mitigation.

Arora and Hastings [39] demonstrated the use of microsegmentation and Zero Trust tactics for minimizing potential attack paths and lowering the extent of damage caused by breaches in cloud infrastructures.

In the end, these new, advanced techniques represent the direction in which cloud and serverless security will be going. Through the mixture of intelligent automation explainability privacy preservation, resilience against adversarial attacks, and constant observability, the research community is developing more robust and flexible security setups capable of dealing with a very complex threat landscape growing day by day.

Comparative Analysis Table Of Existing Approaches

| Paper | Approach | Category | AI Technique | Objective | Advantages | Limitations |
|---|---|---|---|---|---|---|
| Ahmadi 2024 [1] | Security challenges review | Serverless Security | N/A | Threat Identification | Broad Review | No implementation |
| Mahendar 2025 [2] | ML-based IDS survey | Cloud IDS | Machine Learning | ML-based IDS Survey | Broad coverage | No practical evaluation |

| | | | | | | |
|---|---|---|---|---|---|---|
| Othman 2024 [3] | IDS survey | Cloud IDS | Multiple IDS Methods | IDS Classification | Detailed taxonomy | Limited serverless focus |
| Michael 2025 [4] | Best practices review | Cloud IDS | N/A | Deployment Challenges | Practical Insights | No Validation |
| Al-Ghuwairi 2023 [5] | Time-series anomaly detection | AI-based Detection | Machine Learning | Cloud Anomaly Detection | High detection accuracy | Dataset dependency |
| Nguyen 2025 [6] | Silent failure detection | Serverless Anomaly Detection | Anomaly Analysis | Silent Failure Detection | Serverless-specific focus | Limited scalability study |
| Marin 2022 [7] | Security survey | Serverless Security | N/A | Threat Analysis | Strong security overview | No AI integration |
| Dorsett 2025 [8] | DoW attack review | Serverless Security | N/A | DoW Attack Review | Threat Focus | No detection framework |
| Lavi 2024 [9] | Compromised function detection | Serverless IDS | Behavioral Analysis | Compromise Detection | Runtime monitoring | High overhead |
| Xu 2025 [10] | Deep learning survey | AI-based IDS | Deep Learning | DL-based IDS Review | Extensive coverage | Computational complexity |
| Alhusseini 2026 [11] | Hybrid IDS framework | AI-based IDS | Metaheuristic + AI | Intrusion Detection Optimization | Improved accuracy | Early-stage validation |
| Darban 2024 [12] | Time-series survey | Anomaly Detection | Deep Learning | Anomaly Review | Evaluation Framework | Generic domain focus |
| Al-Husseini 2025 [13] | Hybrid IDS | Cloud IDS | Hybrid ML | Security Improvement | Better detection rates | Limited deployment study |
| Siqueira 2025 [14] | Healthcare IDS survey | Domain-specific IDS | AI-based IDS | Healthcare IDS Applications | Sector-specific insights | Limited cloud focus |
| Babaei 2023 [15] | Security review | Cloud Security | Machine Learning | Cloud Security Review | Broad review | No implementation |
| Whitman 2024 [16] | ML anomaly detection | Serverless Detection | Machine Learning | FaaS Anomaly Detection | Serverless relevance | Dataset limitations |
| Islam 2025 [17] | Industry case study | Cloud Anomaly Detection | AI Analytics | Cloud Anomaly Dataset | Real-world validation | Limited serverless focus |
| Li 2025 [18] | FaaSMT framework | Serverless IDS | Lightweight Detection | Serverless IDS Framework | Low overhead | Early-stage evaluation |
| Jegan 2020 [19] | SecLambda | Serverless Security | Runtime Monitoring | Function Protection | Practical framework | Limited scalability |
| Li 2021 [20] | Security survey | Serverless Security | N/A | Security Challenges Review | Comprehensive overview | No experimental work |
| Janumpally 2025 [21] | Privacy review | Serverless Security | N/A | Data Privacy Review | Current challenges identified | No implementation |

| | | | | | | |
|---|---|---|---|---|---|---|
| Lata 2022 [22] | Literature survey | Cloud IDS | IDS Techniques | Future IDS Directions | Research gap analysis | Limited serverless discussion |
| Zhong 2023 [23] | AIOps survey | Anomaly Detection | Time-Series Analysis | AIOps Anomaly Detection | Broad taxonomy | Not cloud-specific |
| Kumar 2024 [24] | Healthcare FaaS security | Serverless Security | N/A | Healthcare FaaS Security | Domain-specific analysis | Limited generalization |
| Ni 2024 [25] | Security quantification | Serverless Security | Risk Modeling | Security Assessment | Security metrics framework | No detection model |
| Yan 2024 [26] | ISSF framework | Cloud-Native Security | DRL Adaptive Learning | Intelligent Security Services | Dynamic defense capability | High complexity |
| Escaleira 2025 [27] | Systematic review | Serverless Security | N/A | Security Mechanisms Review | Comprehensive analysis | No proposed framework |
| Pathade 2026 [28] | AI security analysis | Serverless AI Security | AI Security Models | FaaS AI Protection | Emerging AI threat coverage | Limited validation |
| Paparrizos 2025 [29] | Anomaly detection review | Anomaly Detection | Statistical & ML Methods | Anomaly Evaluation | Evaluation framework | Generic focus |
| Mendes 2023 [30] | XAI review | Explainable AI | Explainable AI | XAI in cybersecurity | Improves transparency | Limited IDS implementation |
| Rjoub 2023 [31] | XAI survey | Explainable AI | Explainable AI | XAI Survey | Better interpretability | Performance trade-offs |
| Khraisat 2024 [32] | Federated IDS survey | Federated Learning IDS | Federated Learning | Federated IDS Survey | Privacy preservation | Communication overhead |
| Agrawal 2021 [33] | FL for IDS | Federated Learning IDS | Federated Learning | FL-based IDS Research | Distributed learning | Resource intensive |
| Alhajjar 2020 [34] | Adversarial ML review | Adversarial Security | Adversarial Learning | Adversarial IDS Attacks | Security awareness | No defense implementation |
| Ennaji 2024 [35] | Adversarial IDS survey | Adversarial Security | Adversarial ML | Adversarial IDS Challenges | Comprehensive review | Limited practical testing |
| Shin 2025 [36] | Bambda framework | Serverless Security | Runtime Verification | Runtime Verification | Continuous monitoring | Performance overhead |
| Borges 2024 [37] | OXN framework | Observability | Automated Assessment | Observability Assessment | Automated analysis | Security focus limited |
| Dkmak 2025 [38] | Night's Watch Algorithm | AI-based Anomaly Detection | Machine Learning | Microservice Anomaly Detection | Cloud-native applicability | Evaluation scope limited |
| Arora 2024 [39] | Microsegmentation architecture | Zero Trust Security | N/A | Zero Trust Framework | Improved isolation | Deployment complexity |
| Li 2025 [40] | SAFE framework | AI-based IDS | Self-Supervised Learning | Self-Supervised IDS | Detects unknown attacks | Training complexity |

## V. RESEARCH GAPS IDENTIFIED FROM THE LITERATURE

The review of the selected forty research papers shows clear progress in serverless security, intrusion detection systems, anomaly detection techniques, and AI-driven cybersecurity frameworks. However, several limitations still prevent the development of strong and practical security solutions for serverless cloud environments. Many existing studies concentrate on traditional cloud infrastructures and offer little support for the dynamic, event-driven nature of serverless computing. Additionally, issues related to real-time threat detection, explainability of AI models, privacy protection, scalability, and resistance to attacks remain largely unsolved. Although recent studies have introduced machine learning, deep learning, federated learning, and cloud-native security frameworks, there is still a lack of integrated, lightweight solutions that are suitable for production-scale deployments. Based on the analysis of the reviewed literature, the main research gaps are organized into the following areas.

### *A. Traditional IDS Limitations*

The various intrusion detection systems surveyed in the literature were not originally designed for serverless environments, but for traditional network and cloud infrastructures. Signature-based methods are frequently ineffective e against zero-day attacks and novel threats, while anomaly-based systems are usually burdened with high false-positive rates. The works of Mahendar and Shivakanth [2], Othman et al. [3] and Lata and Singh [22] demonstrate that existing IDS solutions require heavy modifications to work in serverless architectures. In addition, traditional IDS frameworks are typically based on constant monitoring strategies, which are not compatible with the transient nature of Function-as-a-Service (FaaS) platforms. This limitation highlights the need for adaptive and cloud-native intrusion detection techniques that can operate in highly dynamic settings.

### *B. Lack of Serverless-Specific Detection Models*

Although many studies investigate cloud security and IDPS, very few studies investigate cloud security in a serverless environment. Research by Marin et al. [7], Li et al. [20], Janumpally [21], and Escaleira et al. [27] emphasizes that security mechanisms created for virtual machines and containers cannot be directly used for serverless architectures. The short-lived execution model, state less design, and distributed deployment of serverless functions introduces unique security issues that remain under addressed. Consequently, there is a need for a detector for serverless and event-driven purposes.

### *C. Absence of Real-Time Detection Capabilities*

A number of AI-driven intrusion detection techniques show impressive results in terms of their accuracy during experiments; however, these techniques are devoid of the capability to monitor and respond in real-time. Studies carried out by Al-Ghuwairi et al. [5], Whitman et al. [16], and Dkmak et al. [38] indicate potential in detecting anomalies; however, their practical implementation has yet to be explored. It becomes particularly significant in serverless computing as the time required for an attack and its propagation could be measured in milliseconds.

### *D. High False Positive Rates*

False positives still pose a critical issue in anomaly detection systems. Most ML and DL approaches tend to detect normal behavior modifications as malicious actions, making it more complex to deal with such situations for security analysts. Research findings reported in Xu [10], Darban [12], Zhong [23], and Paparrizos [29] highlight that maintaining a balance between accurate detection and false positives is one of the key challenges in this domain. Too many false positives might cause alert fatigue and slower reaction to attacks.

### *E. Data Availability and Dataset Challenges*

The intrusion detection models based on artificial intelligence require excellent data sets for training and evaluation purposes. Unfortunately, the majority of freely available data sets do not reflect the real serverless workloads. Islam et al. [17] stress the need for large-scale industry data sets. Meanwhile, there have been several references to the problem of absence of benchmark data sets for serverless. The issues of dataset imbalance, outdatedness of the attacks used in the data set, and diversity deficiency persist.

### *F. Lack of Integrated Security Frameworks*

Existing works have focused on various aspects of security, including anomaly detection, intrusion prevention, observability, privacy, or runtime verification. Nevertheless, very few holistic frameworks can integrate the different aspects mentioned above to form an overall framework of security.

Some frameworks, like ISSF [26], OXN [37], or Bambda [36], are good examples; nevertheless, they deal only with some security aspects. The research community lacks overall frameworks that incorporate the different elements discussed above.

### *G. Explainability Issues in AI Models*

Advanced machine learning algorithms are often very complex and non-transparent to users. For example, they cannot explain their decision-making process to humans easily. In their studies, Mendes and Rios [30] and Rjoub et al. [31] underline how essential it is to interpret decision-making in cybersecurity point of view. Cybersecurity experts must be able to understand AI-generated explanations to trust them.

### *H. Privacy and Data Protection Challenges*

Cloud computing environments involve processing of private information for an organization or user, which causes problems related to privacy and compliance with regulatory policies. Despite that, while federated learning techniques proposed by Khraisat et al. [32] and Agrawal et al. [33] try to solve these problems, implementation difficulties arise. The issue of achieving security in intrusion detection systems is still one of the open areas for research.

### *I. Adversarial Vulnerabilities of AI-Based IDS*

Modern investigations show that AI-based intrusion detection systems are also susceptible to adversary attacks. According to Alhajjar et al. [34] and Ennaji et al. [35], it is shown how intruders can take advantage of input manipulation for evasion and deception purposes. The need for an effective method of intrusion detection, which will be resistant to adversary attacks, is becoming a priority. Creating a model of such kind will be one of the tasks for future investigation.

### *J. Summary of Research Gap*

From the literature review, clearly current security measures are not without their problems. Among the challenges identified are: These issues expose the enormous demand for smart scalable explainable, and robust security systems that are tailored for serverless cloud environments.

## VI. FUTURE RESEARCH DIRECTIONS

The uncovered research gaps indicate that there are multiple avenues for developing security solutions in serverless cloud environments. As serverless computing becomes a widespread technology, future research should focus on creating smart, self-adapting, and lightweight security systems that can tackle cyber threats that are constantly changing. The promising research areas in the security of serverless computing, based on the reviewed literature, are, in a way, inspired by the limitations of the present studies.

### *A. Development of Serverless-Specific Intrusion Detection Systems*

In the future, researchers should prioritize the development of intrusion detection systems that are customized for serverless architectures. These differ from conventional cloud infrastructures in that serverless environments are based on event-driven, stateless execution models that require different monitoring methods. So, IDS structures that are simple yet capable of learning the behavior of functions might be a great way to enhance detection and reaction to threats.

### *B. Real-Time AI-Based Threat Detection*

Real-time monitoring of serverless applications is essential for their security. The potential research direction here is creation of very effective ML and DL models which will allow for analyzing the behavior of execution functions in order to detect malicious activity. It can be hypothesized that using streaming analytics together with an artificial intelligence method of detecting malicious code can lead to higher efficiency of the system.

### *C. Explainable Artificial Intelligence for Security Analytics*

Although AI systems are good at detecting things, it is hard to understand how they make their decisions. To fix this, researchers should look into Explainable Artificial Intelligence techniques that give simple explanations for security alerts. This way, security analysts can trust AI-powered cybersecurity solutions and use them more often. AI systems and Explainable Artificial Intelligence techniques can help security analysts. Make AI-powered cybersecurity solutions more popular. Security analysts will trust AI systems more if they understand how AI systems work.

D. Creation of Standardized Serverless Security Datasets

Still, the absence of serverless-targeted datasets available for public use is the main reason that limits the assessment and competitive analysis of security solutions. That is why, in the future, the main concern should be the generation of very realistic benchmark datasets, many attack scenarios, function execution traces, and cloud-native workloads. Such standardized datasets will foster unparalleled performance evaluation, and inevitably, prop innovation in the anomaly detection research domain.

*E. Federated Learning for Privacy-Preserving Security*

Privacy concerns with collecting data in one place can be addressed by using learning. We should look into intrusion detection frameworks that let organizations work together to train models without sharing private data. This way we can make our security better. You should still follow the rules about privacy. Federated learning is a way to address privacy concerns about collecting data in one place. It helps us make our security smarter. It also helps us follow the rules about keeping data private.

*F. Adversarially Robust Detection Models*

We are seeing more and more people trying to attack machine learning systems. So it is very important that we ensure our future security systems can protect against these attacks. We need to do research to make models that can detect when something is not right. These models need to be able to deal with people trying to trick them with data, and also with people trying to sneak past them. Machine learning systems need to be protected from all kinds of attacks. If we can make machine learning systems stronger against attacks, then we can make our cybersecurity solutions better and more reliable. We need to focus on creating machine learning systems that defend against attacks so we can develop better cybersecurity solutions using artificial intelligence.

*G. Integration of Cloud-Native Observability and Security*

With the help of cloud-native platforms, a considerable amount of operational data is being created, which can be very helpful for security analysis. Integrating observability tools, telemetry data, and nuclear detection of the systems could be the way for future research to enhance the visibility of serverless applications. A combination of observability and security analytics may allow us to identify threats proactively, and because of this, the incident response would be quicker.

*H. Zero Trust Security for Serverless Architectures*

Zero Trust principles are a great way to reduce attack surfaces in distributed cloud environments. The next step for researchers is to find out how to implement continuous authentication, microsegmentation, and least-privilege access control in serverless platforms. Combining Zero Trust features with AI-based detection methods can be a very powerful tool to improve security.

*I. Autonomous Security Frameworks Using Artificial Intelligence*

Given the increasing intricacy of cloud infrastructures, the need for higher degrees of automation in cybersecurity operations is emerging. Future studies in this area would do well to be oriented toward independent security setups that are able to identify, evaluate, and respond to threats without the need for a human operator. The integration of reinforcement learning, anomaly detection, and automated response methods might eventually result in serverless security systems that are self-healing and adaptive.

## VII. CONCLUSION

In this review article, a detailed examination of forty research works related to serverless cloud security, intrusion detection systems, anomaly detection methods, artificial intelligence, machine learning, federated learning, explainable AI, and cloud-native security systems was performed. The gathered literature was divided into five main topics: serverless security issues, cloud-based intrusion detection systems, AI and machine learning-based anomaly detection, anomaly detection in serverless environments, and security models for serverless and cloud-native architectures. This division helps to understand, in a more organized way, how modern security solutions are developed in response to the increasing complexity of cloud-native and serverless computing environments.

Some articles dealt with potential security risks of serverless computing, raising issues such as unauthorized access, data leakage, denial-of-service attacks, and function-level breaches while also outlining possible countermeasures. The authors Ahmadi [1] and Marin et al. [7], Li et al. [20], Janumpally [21], and Escaleira et al. [27] argued that it is necessary to create security structures to be exact, tailored to serverless environments. The implementation of intrusion detection systems using machine learning and deep learning models in cloud infrastructures has been explored by Mahendar and Shivakanth [2], Othman et al. [3], Al-Ghuwairi et al. [5], Xu et al. [10], Alhusseini et al. [11], and Al-Husseini [13] indicate that these methods could be highly beneficial in detecting

various forms of cyber-attacks in cloud systems. Besides, the study of abnormality detection techniques by Darban et al. [12], Islam et al. [17], Zhong et al. [23], Paparrizos et al. [29], Borges et al. [37], and Dkmak et al. [38] also unravel the strong potential of AI-enabled methods to discover irregularities and failures in cloud infrastructures at a large scale.

In the security domain of serverless computing, several security architecture proposals have emerged. Jegan et al. [19] suggested SecLambda to ensure security for serverless applications, whereas Li et al. [18] came up with the FaaSMT system, which is capable of lightweight intrusion detection. Also, Yan et al. [26] created the Intelligent Security Service System (ISSF), Shin et al. [36] introduced the Bambda runtime verification setup, and Li et al. [40] came up with the SAFE self-supervised anomaly detection system. Innovative technologies such as Explainable Artificial Intelligence, as covered by Mendes and Rios [30] and Rjoub et al., are discussed. [31], Federated Learning as developed by Khraisat et al. [32] and Agrawal et al. [33], and Zero Trust architectures as advocated by Arora and Hastings [39] confirm the increasing importance of smart and flexible security mechanisms in cloud environments.

But, behind great progress, the literature also reveals several problems to which solutions have not yet been found. For instance, most of the present intrusion detection systems are characterized by a high false-positive rate, lack of explainability, unavailability of serverless-specific datasets, privacy issues, and susceptibility to adversarial attacks. Also, the bulk of the offered solutions continues to concentrate on conventional cloud infrastructures, leaving the peculiarities of serverless computing--such as its transient and stateless nature--inadequately covered.

Taking into account all of what I just said, the research that is to be done in the future should center on the creation of lightweight serverless-specific intrusion detection systems, real-time anomaly detection systems, security models based on explainable AI, privacy-preserving learning methods, adversarially robust architectures, and fully integrated cloud-native security systems. Artificial intelligence coupled with cloud observability, federated learning, and Zero Trust security principles represents a good opportunity for enhancing the security, scalability, and reliability of next-generation serverless cloud applications.

## REFERENCES

[1] S. Ahmadi, “Challenges and Solutions in Network Security for Serverless Computing,” International Journal of Current Science Research and Review, vol. 7, no. 1, pp. 218–229, Jan. 2024, doi: 10.47191/IJCSRR/V7-i1-23.

[2] K. Mahendar and G. Shivakanth, “A Survey of Intrusion Detection Systems Based on Machine Learning for Cloud Security,” International Journal of Electrical and Electronics Engineering, vol. 12, no. 5, pp. 226–242, 2025, doi: 10.14445/23488379/IJEEE-V12I5P119.

[3] S. M. Othman, A. Y. Al-Mutawkkil, and A. M. Alnashi, “Survey of Intrusion Detection Techniques in Cloud Computing,” Sana'a University Journal of Applied Sciences and Technology, vol. 2, no. 4, pp. 363–374, 2024, doi: 10.59628/jast.v2i4.970.

[4] D. Michael, “Cloud-based Intrusion Detection Systems: Challenges and Best Practices,” Jul. 2025. [Online]. Available: https://www.researchgate.net/publication/393801749_Cloud-based_Intrusion_Detection_Systems_Challenges_and_Best_Practices

[5] A.-R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, “Intrusion Detection in Cloud Computing Based on Time Series Anomalies Utilizing Machine Learning,” Journal of Cloud Computing, vol. 12, no. 1, article 127, Aug. 2023, doi: 10.1186/s13677-023-00491-x.

[6] C. Nguyen, E. Elmroth, and M. Bhuyan, “Silent Failures in Stateless Systems: Rethinking Anomaly Detection for Serverless Computing,” in Proc. IEEE Int. Conf. Service-Oriented System Engineering (SOSE), Tucson, AZ, USA, 2025, pp. 8–19, doi: 10.1109/SOSE67019.2025.00006.

[7] E. Marin, D. Perino, and R. Di Pietro, “Serverless Computing: A Security Perspective,” arXiv preprint arXiv:2107.03832, 2022, doi: 10.48550/arXiv.2107.03832.

[8] M. Dorsett, S. Mann, J. Chowdhury, and A. Mahmood, “A Comprehensive Review of Denial of Wallet Attacks in Serverless Architectures,” arXiv preprint arXiv:2508.19284, 2025, doi: 10.48550/arXiv.2508.19284.

[9] D. Lavi, O. Brodt, D. Mimran, Y. Elovici, and A. Shabtai, “Detection of Compromised Functions in a Serverless Cloud Environment,” arXiv preprint arXiv:2408.02641, 2024, doi: 10.48550/arXiv.2408.02641.

[10] Z. Xu, Y. Wu, S. Wang, J. Gao, T. Qiu, Z. Wang, H. Wan, and X. Zhao, “Deep Learning-based Intrusion Detection Systems: A Survey,” ACM Computing Surveys, vol. 58, no. 1, article 1, pp. 1–38, Oct. 2025.

[11] M. M. Alhusseini, A. Rouhi, and M.-R. Feizi-Derakhshi, “AI-Powered Hybrid Intrusion Detection Framework for Cloud Security Using Novel Metaheuristic Optimization,” arXiv preprint arXiv:2601.01134, 2026, doi: 10.48550/arXiv.2601.01134.

[12] Z. Z. Darban, G. I. Webb, S. Pan, C. C. Aggarwal, and M. Salehi, “Deep Learning for Time Series Anomaly Detection: A Survey,” ACM Computing Surveys, vol. 57, no. 11, article 338, pp. 1–42, 2024, doi: 10.1145/3691338.

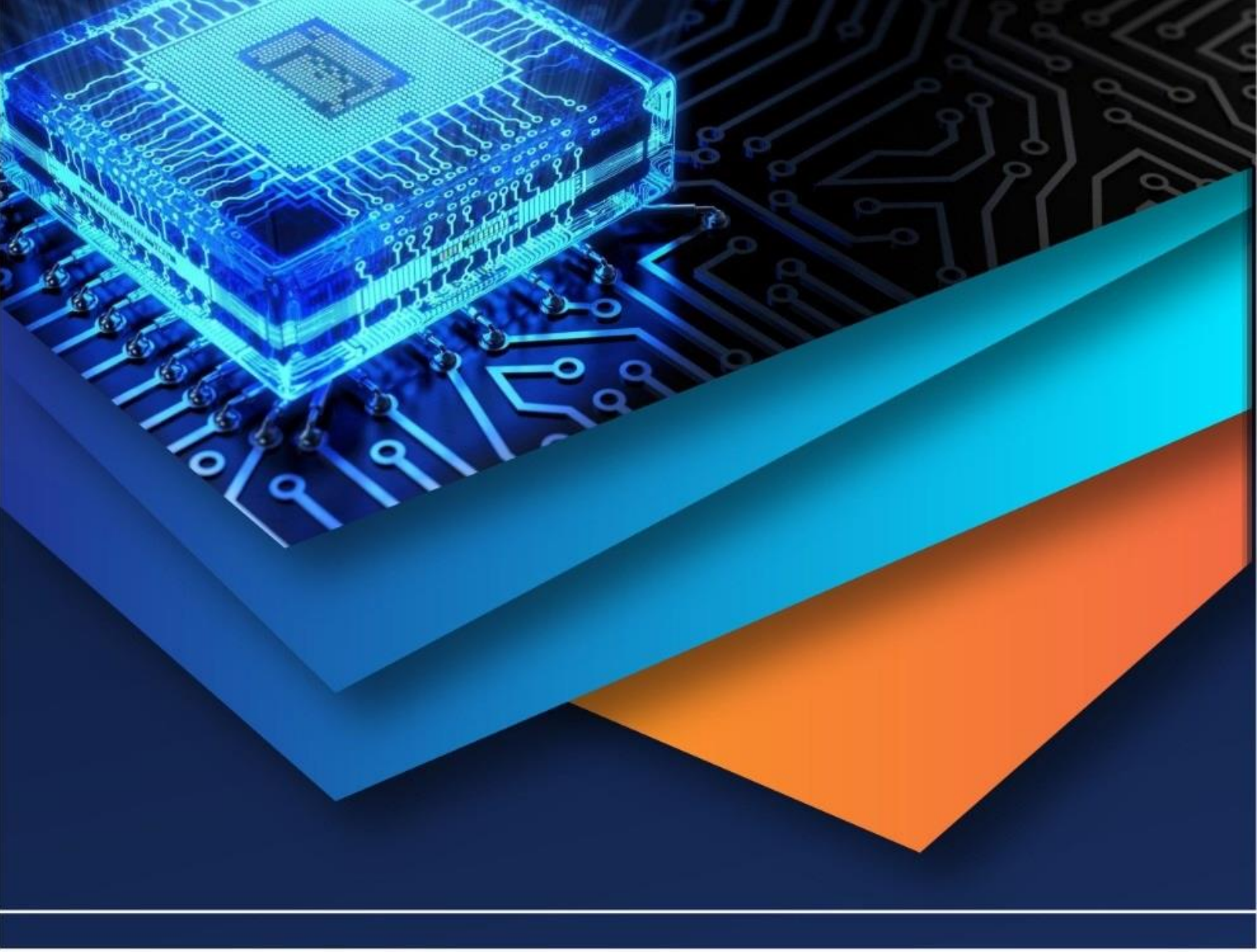
[13] M. M. Al-Husseini, “A Hybrid Intrusion Detection System with a New Approach to Protect the Cybersecurity of Cloud Computing,” arXiv preprint arXiv:2506.19934, 2025, doi: 10.48550/arXiv.2506.19934.

[14] L. P. Siqueira, C. L. Batista, P. H. Lui, J. F. Kazienko, S. E. Quincozes, V. E. Quincozes, D. Welfer, and S. Nomura, “A Comprehensive Survey on Intrusion Detection Systems for Healthcare 5.0: Concepts, Challenges, and Practical Applications,” Sensors, vol. 25, no. 20, article 6261, 2025, doi: 10.3390/s25206261.

[15] A. Babaei, P. M. Kebria, M. M. Dalvand, and S. Nahavandi, “A Review of Machine Learning-based Security in Cloud Computing,” arXiv preprint arXiv:2309.04911, 2023, doi: 10.48550/arXiv.2309.04911.

[16] J. Whitman, A. El-Karim, P. Nandakumar, F. Ortega, and L. Zheng, “Machine Learning for Anomaly Detection in Serverless Cloud Computing,” Oct. 2024. [Online]. Available: https://www.researchgate.net/publication/391498025_Machine_Learning_for_Anomaly_Detection_in_Serverless_Cloud_Computing

[17] M. S. Islam, M. S. Rakha, W. Pourmajidi, J. Sivaloganathan, J. Steinbacher, and A. Miranskyy, "Anomaly Detection in Large-Scale Cloud Systems: An Industry Case and Dataset," in Proc. 2025 IEEE/ACM 47th Int. Conf. Software Engineering: Software Engineering in Practice (ICSE-SEIP), Ottawa, ON, Canada, 2025, doi: 10.1109/ICSE-SEIP66354.2025.00039.
[18] C. Li, L. Huang, D. He, Y. Wen, G. Liu, and L. Duan, "FaaSMT: Lightweight Serverless Framework for Intrusion Detection Using Merkle Tree and Task Inlining," arXiv preprint arXiv:2503.06532, 2025, doi: 10.48550/arXiv.2503.06532.
[19] D. S. Jegan, L. Wang, S. Bhagat, T. Ristenpart, and M. Swift, "Guarding Serverless Applications with SecLambda," arXiv preprint arXiv:2011.05322, 2020, doi: 10.48550/arXiv.2011.05322.
[20] X. Li, X. Leng, and Y. Chen, "Securing Serverless Computing: Challenges, Solutions, and Opportunities," arXiv preprint arXiv:2105.12581, 2021, doi: 10.48550/arXiv.2105.12581.
[21] [B. K. R. Janumpally, "A Review on Data Security and Privacy in Serverless Computing: Key Strategies, Emerging Challenges," International Journal of Innovative Science and Research Technology, vol. 10, no. 3, pp. 118–126, Mar. 2025, doi: 10.38124/ijisrt/25mar023.
[22] S. Lata and D. Singh, "Intrusion Detection System in Cloud Environment: Literature Survey & Future Research Directions," International Journal of Information Management Data Insights, vol. 2, no. 2, article 100134, Nov. 2022, doi: 10.1016/j.jjimei.2022.100134.
[23] Z. Zhong, Q. Fan, J. Zhang, M. Ma, S. Zhang, Y. Sun, Q. Lin, Y. Zhang, and D. Pei, "A Survey of Time Series Anomaly Detection Methods in the AIOps Domain," arXiv preprint arXiv:2308.00393, 2023, doi: 10.48550/arXiv.2308.00393.
[24] S. Kumar, "Overcoming Security Obstacles in Serverless Function-as-a-Service (FaaS) for Healthcare Insurance," International Journal of Computer Trends and Technology, vol. 72, no. 10, pp. 86–93, Oct. 2024, doi: 10.14445/22312803/IJCTT-V72I10P114.
[25] K. Ni, S. K. Mondal, H. M. D. Kabir, T. Tan, and H.-N. Dai, "Toward Security Quantification of Serverless Computing," Journal of Cloud Computing, vol. 13, no. 1, article 140, pp. 1–27, 2024, doi: 10.1186/s13677-024-00703-y.
[26] Y. Yan, K. Huang, and M. Siegel, "ISSF: The Intelligent Security Service Framework for Cloud-Native Operation," arXiv preprint arXiv:2403.01507, 2024, doi: 10.48550/arXiv.2403.01507.
[27] P. Escaleira, V. A. Cunha, J. P. Barraca, D. Gomes, and R. L. Aguiar, "A Systematic Review on Security Mechanisms for Serverless Computing," Cluster Computing, vol. 28, art. no. 465, 2025, doi: 10.1007/s10586-025-05371-4.
[28] C. Pathade, V. Dhimam, S. Ahmad, and I. Lareb, "Serverless AI Security: Attack Surface Analysis and Runtime Protection Mechanisms for FaaS-Based Machine Learning," arXiv preprint arXiv:2601.11664, 2026, doi: 10.48550/arXiv.2601.11664.
[29] J. Paparrizos, P. Boniol, Q. Liu, and T. Palpanas, "Advances in Time-Series Anomaly Detection: Algorithms, Benchmarks, and Evaluation Measures," in Proc. 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '25), Toronto, ON, Canada, Aug. 2025, pp. 6151–6161, doi: 10.1145/3711896.3736565.
[30] C. F. D'Almeida e Mendes and T. N. Rios, "Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review," arXiv preprint arXiv:2303.01259, 2023, doi: 10.48550/arXiv.2303.01259.
[31] G. Rjoub, J. Bentahar, O. Abdel Wahab, R. Mizouni, A. Song, R. Cohen, H. Otrok, A. Mourad, and D. R. Cheriton, "A Survey on Explainable Artificial Intelligence for Cybersecurity," arXiv preprint arXiv:2303.12942, 2023, doi: 10.48550/arXiv.2303.12942.
[32] A. Khraisat, A. Alazab, S. Singh, T. Jan, and A. J. Gomez, "Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions," ACM Computing Surveys, vol. 57, no. 1, article 7, pp. 1–38, Oct. 2024, doi: 10.1145/3687124.
[33] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions," arXiv preprint arXiv:2106.09527, 2021, doi: 10.48550/arXiv.2106.09527.
[34] E. Alhajjar, P. Maxwell, and N. D. Bastian, "Adversarial Machine Learning in Network Intrusion Detection Systems," arXiv preprint arXiv:2004.11898, 2020, doi: 10.48550/arXiv.2004.11898.
[35] S. Ennaji, F. De Gaspari, D. Hitaj, A. K. Bidi, and L. V. Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," arXiv preprint arXiv:2409.18736, 2024, doi: 10.48550/arXiv.2409.18736.
[36] C. Shin, B. Kim, and S. Lee, "Bambda: A Real-Time Verification Framework for Serverless Computing," IEEE Access, vol. 13, pp. 1–1, 2025, doi: 10.1109/ACCESS.2025.3572729.
[37] M. C. Borges, J. Bauer, and S. Werner, "OXN -- Automated Observability Assessments for Cloud-Native Applications," in Proc. 21st IEEE International Conference on Software Architecture (ICSA), Poster Track, 2024, doi: 10.1109/ICSA-C63560.2024.00035.
[38] G. Dkmak, B. Can, O. Sevinc, C. B. Egeli, F. Baday, and B. Cetintav, "AI-Driven Anomaly Detection in Cloud-Native Microservices: The Night's Watch Algorithm," Applied Sciences, vol. 15, no. 23, article 12762, 2025, doi: 10.3390/app152312762.
[39] S. Arora and J. Hastings, "Microsegmented Cloud Network Architecture Using Open-Source Tools for a Zero Trust Foundation," in Proc. IEEE International Conference on Security of Information and Networks (SIN), 2024, doi: 10.1109/SIN63213.2024.10871361.
[40] E. Li, Z. Shang, O. Gungor, and T. Rosing, "SAFE: Self-Supervised Anomaly Detection Framework for Intrusion Detection," arXiv preprint arXiv:2502.07119, 2025, doi: 10.48550/arXiv.2502.07119.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY