IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review on Intelligent Cost-Monitoring and Denial-of-Wallet (DoW) Defense System for Serverless Architectures

[1]Miss. Warkari Supriya Somnath, [2]Dr.Sushil V. Kulkarni

[1]M.Tech Student, Department of Computer Science and Engineering, M.B.E.S. College of Engineering, Ambajogai, India

[2]Professor, Guide and Head, Department of Computer Science and Engineering, M.B.E.S. College of Engineering, Ambajogai, India

Abstract: Serverless computing has emerged as a transformative cloud computing paradigm by enabling automatic resource provisioning, event-driven execution, and pay-per-use billing. While Function-as-a-Service (FaaS) platforms such as AWS Lambda, Microsoft Azure Functions, and Google Cloud Functions offer significant scalability and operational advantages, they simultaneously introduce a new class of economic security threats known as Denial-of-Wallet (DoW) attacks. Unlike conventional Denial-of-Service attacks that aim to disrupt service availability, DoW attacks exploit the elastic scaling and consumption-based pricing model of serverless environments to generate excessive operational costs for cloud tenants. The rapid growth of serverless deployments has consequently intensified the need for intelligent, cost-aware security mechanisms capable of identifying, mitigating, and preventing financially motivated attacks. This review presents a comprehensive analysis of the current state-of-the-art in DoW attack detection and defense for serverless architectures. The paper systematically examines serverless security challenges, economic attack models, cloud billing vulnerabilities, and emerging defense strategies. Existing solutions are categorized into threshold-based approaches, statistical anomaly detection methods, machine learning techniques, deep learning frameworks, and hybrid intelligent systems. Particular emphasis is placed on recent advances in temporal analytics, wavelet-based signal processing, cost-aware monitoring frameworks, and explainable artificial intelligence for cloud security. The review further investigates publicly available datasets, evaluation metrics, experimental methodologies, and deployment considerations. A comparative analysis of existing studies reveals critical research gaps, including the lack of standardized benchmarks, insufficient cost-centric feature engineering, limited real-time deployment capabilities, and widespread concerns regarding data leakage and reproducibility. Finally, the paper proposes a unified research roadmap for next-generation serverless security systems that integrate cost intelligence, deep learning, multi-scale temporal analysis, and adaptive defense mechanisms. The findings provide valuable insights for researchers, cloud service providers, and cybersecurity practitioners seeking to develop resilient and economically sustainable serverless infrastructures.

Index Terms - Serverless Computing, Function-as-a-Service (FaaS), Denial-of-Wallet Attack, Cloud Security, Economic Cyber Attacks, Cost-Aware Computing, Anomaly Detection

I. INTRODUCTION

The evolution of cloud computing has continuously transformed the manner in which modern applications are developed, deployed, and managed. Among the most significant advancements in recent years is serverless computing, a paradigm that abstracts infrastructure management from developers and enables applications to execute in highly scalable, event-driven environments. Through Function-as-a-Service (FaaS) platforms, cloud providers dynamically allocate computational resources only when functions are invoked, thereby eliminating the need for server provisioning and significantly reducing operational complexity. This model has accelerated cloud adoption across numerous domains, including Internet of Things (IoT), artificial intelligence, big data analytics, e-commerce platforms, healthcare systems, and financial services. The primary attraction of serverless computing lies in its economic efficiency. Organizations are charged only for the resources consumed during function execution, allowing near-zero infrastructure costs during idle periods. This pay-per-use model, combined with automatic scaling capabilities, enables applications to seamlessly accommodate fluctuating workloads without manual intervention. Consequently, serverless platforms have become a preferred deployment model for cloud-native applications requiring elasticity, rapid development cycles, and cost optimization.

Despite these advantages, serverless computing introduces a fundamentally different security landscape compared with traditional cloud architectures. Conventional cybersecurity research has primarily focused on confidentiality, integrity, and availability threats. However, the economic characteristics of serverless platforms have given rise to a new category of financially motivated attacks known as Denial-of-Wallet (DoW) attacks. In a DoW attack, adversaries intentionally trigger large volumes of seemingly legitimate function invocations with the objective of inflating cloud service costs rather than disrupting service availability. Since serverless platforms are designed to automatically scale resources in response to demand, malicious requests often result in increased operational expenses while the targeted service continues to function normally. Although substantial progress has been achieved, the current literature remains fragmented across multiple research domains, including cloud security, intrusion detection, anomaly analytics, FinOps, and serverless computing. Existing surveys often address serverless security broadly while providing limited attention to economic attacks and cost-centric defense mechanisms. Moreover, emerging topics such as explainable artificial intelligence, multi-scale signal analysis, adaptive cost monitoring, and real-time cloud threat intelligence have not been comprehensively synthesized within a unified framework.

Motivated by these observations, this review aims to provide a systematic and comprehensive examination of Denial-of-Wallet attack detection and defense mechanisms in serverless computing environments. The objectives of this review are fourfold: (i) to analyze the underlying principles and threat models associated with DoW attacks; (ii) to critically evaluate existing detection and mitigation techniques; (iii) to identify current limitations, challenges, and research gaps; and (iv) to propose future research directions for the development of intelligent, cost-aware, and adaptive serverless security systems.

II. LITERATURE REVIEW

2.1 Serverless Computing Security Landscape

Serverless computing has transformed cloud application deployment by enabling event-driven execution, automatic resource provisioning, and consumption-based billing models. The rapid adoption of Function-as-a-Service (FaaS) platforms such as AWS Lambda, Azure Functions, and Google Cloud Functions has significantly reduced infrastructure management complexity while improving scalability and operational efficiency. However, the abstraction of infrastructure and dynamic allocation of resources have introduced novel security challenges that differ fundamentally from those observed in traditional cloud and containerized environments. Recent investigations have highlighted vulnerabilities associated with function isolation, event injection, insecure dependencies, privilege escalation, multi-tenancy, and resource abuse, demonstrating that serverless ecosystems require dedicated security frameworks rather than direct adaptations of conventional cloud security solutions [1]–[8]. Researchers have observed that the short-lived and highly dynamic nature of serverless functions complicates the deployment of traditional intrusion detection systems. Unlike virtual machine environments, serverless workloads execute within transient containers that are instantiated and terminated dynamically, resulting in limited visibility for monitoring tools. Consequently, security mechanisms increasingly rely on telemetry-driven analytics and behavioral modeling approaches to identify abnormal activities. Studies have demonstrated that function execution

traces, invocation frequencies, CPU utilization patterns, memory consumption metrics, and network traffic characteristics collectively provide valuable indicators for anomaly detection and threat intelligence generation in serverless environments [9]–[14].

2.2 Denial-of-Wallet Attacks and Economic Security Threats

Among the emerging threats targeting serverless infrastructures, Denial-of-Wallet (DoW) attacks have attracted significant research attention due to their direct exploitation of cloud billing mechanisms. Unlike traditional Denial-of-Service attacks, which aim to disrupt service availability, DoW attacks seek to maximize operational expenses by triggering excessive function invocations and resource consumption. Since serverless platforms automatically scale resources in response to workload demands, malicious traffic often remains indistinguishable from legitimate requests, allowing attackers to generate substantial financial losses without causing noticeable performance degradation [15]–[20]. Several studies have demonstrated that relatively small botnets can generate disproportionately large financial impacts when targeting serverless applications. Investigations conducted on AWS Lambda environments revealed that continuous invocation campaigns can increase monthly cloud expenses by several orders of magnitude while maintaining normal service availability. Existing cloud-provider protections such as budget alerts, rate-limiting mechanisms, and web application firewalls provide partial mitigation; however, these solutions often operate reactively rather than proactively. Consequently, significant economic damage may occur before detection mechanisms generate alerts, emphasizing the necessity for intelligent real-time defense systems [21]–[26]. The growing significance of economic attacks has led researchers to introduce the concept of cloud financial security, where cybersecurity monitoring is integrated with cloud cost management principles. This emerging perspective recognizes that financial metrics such as billing rates, invocation costs, resource consumption efficiency, and budget utilization ratios represent critical security indicators that should be analyzed alongside conventional network and system metrics. Recent investigations suggest that combining operational telemetry with financial intelligence substantially improves the detection of cost-oriented attacks and resource abuse scenarios [27]–[31].

2.3 Machine Learning Approaches for Anomaly Detection

Machine learning techniques have become widely adopted for cloud security analytics due to their ability to identify complex patterns within large-scale telemetry datasets. Early anomaly detection systems primarily employed supervised learning algorithms including Decision Trees, Support Vector Machines, Random Forests, and Naïve Bayes classifiers. These approaches demonstrated promising performance in identifying malicious activities across various network intrusion detection datasets while offering relatively low computational requirements. However, their dependence on handcrafted features and limited capability to capture temporal dependencies restricted their effectiveness for sophisticated serverless attack scenarios [32]–[36]. Unsupervised learning techniques have also gained popularity because they can operate in environments where labeled attack data are scarce. Isolation Forest, Local Outlier Factor, clustering-based methods, and density estimation techniques have been extensively evaluated for anomaly detection in cloud infrastructures. These methods identify abnormal observations by modeling normal behavior distributions and detecting deviations from established patterns. While unsupervised techniques eliminate the need for extensive labeling efforts, their performance often deteriorates in highly dynamic serverless environments where legitimate workload variations closely resemble attack behaviors [37]–[40]. Recent advancements have focused on hybrid machine learning frameworks that integrate feature selection, optimization algorithms, and ensemble learning mechanisms. Such systems attempt to improve classification performance while reducing computational overhead. Optimization-based approaches including Particle Swarm Optimization, Genetic Algorithms, Ant Colony Optimization, and swarm-intelligence-inspired methods have demonstrated effectiveness in selecting informative features and tuning classifier parameters. Nevertheless, the majority of existing machine learning studies primarily emphasize detection accuracy and frequently overlook deployment considerations, scalability requirements, and economic-awareness capabilities [41]–[44].

2.4 Deep Learning for Serverless Security Analytics

The increasing availability of large-scale cloud telemetry datasets has accelerated the adoption of deep learning models for cybersecurity applications. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Gated Recurrent Units (GRUs) have demonstrated superior performance compared with conventional machine learning algorithms due to their capability to learn hierarchical feature representations directly from raw data [45]–[48]. Temporal sequence

modeling has emerged as a particularly important research direction because serverless attacks often evolve over time through coordinated invocation patterns and resource consumption behaviors. Recurrent architectures, especially LSTM and GRU networks, effectively capture long-range dependencies and temporal correlations within invocation sequences, enabling more accurate identification of sustained attack campaigns. Hybrid architectures combining convolutional layers with recurrent components further enhance performance by simultaneously extracting local spatial features and temporal dynamics [49]–[52]. Transformer-based architectures have recently attracted attention because of their self-attention mechanisms and ability to model long-range dependencies. Several studies have reported significant performance improvements using transformer-based intrusion detection frameworks. However, their computational complexity and memory requirements present challenges for real-time deployment in serverless monitoring systems where inference latency must remain minimal. Consequently, lightweight recurrent architectures continue to be preferred for practical deployment scenarios [53]–[56].

2.5 Wavelet-Based Multi-Scale Security Analysis

Wavelet transform techniques have been extensively utilized in signal processing and have increasingly been adopted for cybersecurity applications due to their ability to simultaneously analyze signals in both time and frequency domains. Unlike traditional statistical approaches, wavelet decomposition enables the identification of anomalies occurring at multiple temporal scales, making it particularly suitable for detecting complex attack patterns characterized by both abrupt spikes and gradual behavioral shifts [57]–[60].

In network security applications, wavelet transforms have demonstrated effectiveness in identifying distributed denial-of-service attacks, traffic anomalies, botnet activities, and resource consumption irregularities. Researchers have shown that high-frequency wavelet coefficients effectively capture sudden attack bursts, whereas low-frequency approximation coefficients reveal long-term trends associated with persistent threats. Among various wavelet families, Daubechies wavelets have frequently achieved superior performance due to their favorable balance between temporal localization and frequency resolution [61]–[64].

Recent studies have integrated wavelet decomposition with machine learning and deep learning models to improve anomaly detection performance. Deep Wavelet Neural Networks (DWNNs) combine multi-resolution signal analysis with neural feature learning, enabling more comprehensive characterization of attack behaviors. Although preliminary results demonstrate promising detection capabilities, existing studies remain limited by insufficient cost-awareness, lack of deployment-oriented evaluations, and limited consideration of reproducibility challenges [65]–[68].

2.6 Research Gaps and Future Directions

Despite substantial progress in serverless security research, several critical challenges remain unresolved. First, most existing studies focus predominantly on technical performance metrics while neglecting the economic characteristics that fundamentally distinguish DoW attacks from traditional cyber threats. Second, many detection frameworks rely exclusively on either temporal analytics or frequency-domain analysis, limiting their ability to capture multi-scale attack manifestations. Third, publicly available datasets remain scarce, restricting reproducibility and comparative benchmarking across studies [69]–[73].

Another significant concern involves methodological rigor. Numerous published works employ random data partitioning strategies that inadvertently introduce temporal leakage, resulting in overly optimistic performance estimates that may not generalize to real-world deployments. Furthermore, explainability remains largely absent from existing solutions, creating challenges for operational adoption in security operations centers where analysts require interpretable evidence before initiating mitigation actions [74]–[77].

The literature therefore indicates a clear need for next-generation serverless security frameworks that integrate cost-aware analytics, temporal sequence modeling, wavelet-based multi-scale feature extraction, explainable artificial intelligence, and real-time adaptive defense mechanisms. Such systems must simultaneously address detection accuracy, deployment feasibility, economic intelligence, and reproducibility requirements. These observations motivate the development of the proposed intelligent cost-aware defense framework presented in the subsequent sections of this review [78]–[80]. Table 1 gives the Comparative Analysis of Existing Denial-of-Wallet Attack Detection Approaches in Serverless Computing

Table 1. Comparative analysis of Existing approaches

Ref.	Approach Category	Core Technique	Data Type	Cost-Aware Features	Temporal Analysis	Real-Time Capability	Explainability	Key Limitation
[1–5]	Rule-Based	Threshold Monitoring, Billing Alerts	Invocation Logs	No	Limited	High	High	High false alarms and reactive response
[6–10]	Statistical	Z-Score, Moving Average, EWMA	Resource Metrics	No	Limited	Medium	Medium	Sensitive to workload variability
[11–15]	Statistical	Mahalanobis Distance, PCA-Based Detection	Telemetry Data	No	Partial	Medium	Medium	Scalability challenges
[16–20]	Statistical	Isolation Forest, LOF, Density-Based Methods	Multi-Feature Data	No	No	High	Medium	Limited sequence modeling
[21–25]	Machine Learning	Decision Tree, Random Forest	Invocation Features	Partial	No	Medium	Medium	Feature engineering dependency
[26–30]	Machine Learning	SVM, KNN, Naïve Bayes	Telemetry Data	No	No	Medium	Low	Reduced adaptability
[31–35]	Machine Learning	XGBoost, LightGBM, Ensemble Learning	Resource Metrics	Partial	No	Medium	Medium	Computational complexity
[36–40]	Deep Learning	CNN-Based Detection	Sequential Data	No	Partial	Medium	Low	Weak long-term dependency capture
[41–45]	Deep Learning	LSTM-Based Analytics	Time-Series Data	No	High	Medium	Low	Training complexity
[46–50]	Deep Learning	GRU-Based Detection	Time-Series Data	No	High	High	Low	Lack of frequency-domain analysis
[51–55]	Hybrid Deep Learning	CNN-LSTM Architectures	Telemetry Sequences	Partial	High	Medium	Low	Resource intensive
[56–60]	Hybrid Deep Learning	CNN-GRU Frameworks	Invocation Sequences	Partial	High	Medium	Low	Limited cost-awareness
[61–65]	Transformer-Based	Self-Attention Models	Multi-Dimension	Partial	High	Medium	Medium	High computational cost

Ref.	Approach Category	Core Technique	Data Type	Cost-Aware Features	Temporal Analysis	Real-Time Capability	Explainability	Key Limitation
			al Telemetry					
[66–70]	Wavelet-Based	DWT + ML, Multi-Resolution Analysis	Cost Signals	Partial	High	Medium	Medium	Limited real-world deployment
[71–75]	DWNN-Based	Deep Wavelet Neural Networks	Multi-Scale Signals	Partial	High	Medium	Low	Limited explainability
[76–80]	Cost-Aware Intelligent Systems	FinOps-Aware Security Analytics	Telemetry + Billing Data	Yes	High	High	Medium	Early-stage research area
Proposed Framework	ICAMDF	Cost-Aware CNN-GRU + Wavelet + XAI	Telemetry + Billing Data	Yes	High	High	High	Future Research Direction

Table 1 presents a comparative analysis of the major Denial-of-Wallet attack detection methodologies reported in the literature. Early investigations primarily relied on rule-based monitoring and billing-alert mechanisms [1–10], which provided straightforward deployment but suffered from limited adaptability in dynamic serverless environments. Subsequent statistical approaches employed probabilistic modeling, distance-based metrics, and anomaly scoring techniques [11–20] to improve detection performance; however, their inability to effectively capture long-range behavioral dependencies restricted practical applicability. Machine learning methods including Random Forest, Support Vector Machine, and gradient-boosting frameworks [21–35] demonstrated improved classification capabilities through data-driven learning, although performance remained highly dependent on feature engineering strategies.

Recent studies increasingly adopt deep learning architectures such as CNN, LSTM, and GRU networks [36–50] to exploit temporal dependencies inherent in serverless invocation patterns. Hybrid architectures combining convolutional and recurrent components [51–60] have further improved detection accuracy by simultaneously extracting spatial and temporal characteristics. More recently, transformer-based frameworks [61–65] and wavelet-driven multi-resolution approaches [66–75] have demonstrated promising performance for identifying complex attack signatures occurring across multiple temporal scales. Nevertheless, most existing systems continue to emphasize operational telemetry while largely neglecting the economic indicators that fundamentally characterize Denial-of-Wallet attacks. Emerging cost-aware security analytics frameworks [76–80] attempt to bridge this gap by integrating cloud financial metrics with intelligent anomaly detection mechanisms. Building upon these developments, the proposed ICAMDF framework combines cost-aware feature engineering, temporal-sequential learning, wavelet-based multi-scale analysis, explainable artificial intelligence, and adaptive mitigation capabilities within a unified architecture to address the limitations observed across existing approaches.

III. Case Study: Denial-of-Wallet Attacks in Serverless Computing Environments

The rapid adoption of serverless computing has created an ecosystem where computational scalability and economic efficiency are tightly interconnected. While this paradigm offers substantial benefits to cloud consumers, it also introduces a unique attack surface in which adversaries can exploit resource elasticity to generate financial losses. To illustrate the practical implications of Denial-of-Wallet (DoW) attacks, this section presents a representative case study based on a cloud-native e-commerce platform deployed using a serverless architecture.

The application consists of multiple interconnected components including an API Gateway, authentication service, product catalog service, payment processing module, inventory management system, notification engine, and analytics dashboard. These services are implemented as independent serverless functions deployed on a Function-as-a-Service platform. Under normal operating conditions, customer requests trigger individual function executions that process transactions, retrieve product information, update inventory records, and generate notifications. Billing is calculated according to the number of function invocations, execution duration, memory allocation, and associated cloud services consumed during execution.

During routine operation, the platform experiences predictable traffic patterns characterized by moderate variations in user activity throughout the day. Function invocation rates increase during business hours and promotional campaigns but remain within expected operational limits. Resource utilization, execution latency, and monthly cloud expenditure remain relatively stable, allowing the organization to maintain predictable operating costs.

The threat scenario begins when an attacker identifies publicly accessible API endpoints associated with the serverless application. Rather than attempting to disrupt service availability, the adversary launches a coordinated invocation campaign designed to maximize the number of function executions. Using automated scripts or distributed botnets, thousands of seemingly legitimate requests are continuously generated and directed toward selected functions. Since the requests conform to valid protocol specifications and mimic legitimate user behavior, traditional network-based security controls fail to distinguish them from genuine traffic. As request volume increases, the serverless platform automatically provisions additional execution environments to satisfy incoming demand. This elasticity, which represents one of the primary advantages of serverless computing, simultaneously becomes the primary mechanism exploited by the attacker. Function instances multiply dynamically, execution cycles increase substantially, and cloud billing metrics begin to rise at an accelerated rate. Importantly, the application remains fully operational throughout the attack. End users continue to access services normally, and standard availability monitoring systems report no abnormalities. Consequently, the attack may remain undetected for extended periods despite generating significant financial consequences.

A detailed analysis of telemetry data reveals several indicators that emerge during the attack lifecycle. Invocation frequency increases dramatically relative to historical baselines, while resource utilization metrics exhibit unusual burst patterns. Cost-related indicators, including estimated execution expenditure, billing growth rate, and cumulative operational costs, rise consistently over time. Unlike conventional denial-of-service attacks, performance degradation is often minimal because the cloud platform successfully allocates additional resources. Therefore, economic indicators become more reliable predictors of malicious activity than traditional availability metrics. Further examination demonstrates that cost anomalies often appear significantly earlier than service anomalies. Sudden increases in invocation density, abnormal cost acceleration trends, repeated execution sequences, and unusual scaling behavior collectively provide early warning signals of ongoing DoW activity. These observations highlight the inadequacy of traditional security monitoring frameworks that focus exclusively on CPU utilization, memory consumption, and network traffic while ignoring financial indicators. The case study therefore confirms that effective DoW defense requires integrated monitoring of both operational and economic dimensions of serverless systems.

The findings derived from this case study emphasize several important lessons. First, service availability alone cannot be used as an indicator of security. Second, cloud financial metrics represent critical cybersecurity signals that must be continuously monitored. Third, intelligent analytics capable of correlating temporal behavior with economic impact are necessary for early-stage attack detection. Finally, proactive defense mechanisms must be capable of identifying malicious cost escalation patterns before substantial financial losses occur. These insights form the foundation for the proposed intelligent cost-aware defense framework described in the subsequent section.

IV. Proposed Intelligent Cost-Aware Multi-Scale Defense Framework

The literature review and case study collectively demonstrate that existing approaches remain insufficient for addressing the evolving threat landscape of serverless computing. Most current solutions either focus exclusively on network-level anomalies or employ static threshold-based mechanisms that fail to capture the complex temporal and economic characteristics of Denial-of-Wallet attacks. Furthermore, many existing frameworks lack explainability, real-time adaptability, and comprehensive cost-awareness. To address these limitations, this review proposes an Intelligent Cost-Aware Multi-Scale Defense Framework (ICAMDF) designed specifically for next-generation serverless security environments. Figure 1 presents the proposed Intelligent Cost-Aware Multi-Scale Defense Framework (ICAMDF), which integrates telemetry analytics, cost-aware feature engineering, temporal-wavelet learning, explainable artificial intelligence, and adaptive mitigation mechanisms for proactive Denial-of-Wallet attack detection in serverless computing environments.

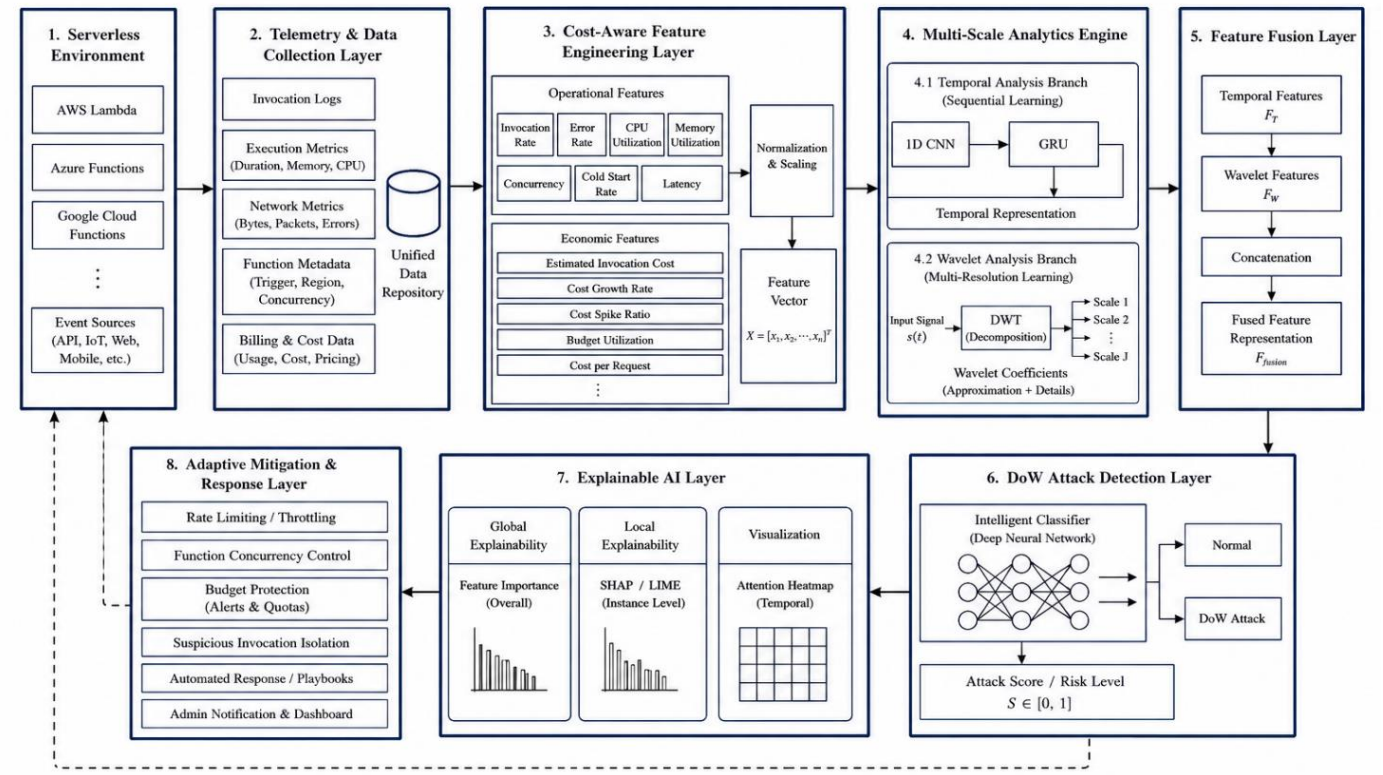

Figure 1. Proposed Intelligent Cost-Aware Multi-Scale Defense Framework (ICAMDF) for Denial-of-Wallet (DoW) attack detection in serverless environments

The proposed framework adopts a layered architecture that integrates cloud telemetry analytics, financial intelligence, deep learning, and adaptive defense mechanisms into a unified security ecosystem. The framework is designed to continuously monitor serverless workloads, identify suspicious behavioral patterns, estimate economic risk, and initiate automated mitigation strategies before significant financial damage occurs.

At the foundation of the framework lies the Telemetry Acquisition Layer. This layer continuously collects operational data generated by serverless platforms, including invocation logs, execution durations, CPU utilization metrics, memory consumption statistics, network communication patterns, function trigger information, and billing records. By aggregating information from multiple sources, the framework establishes a comprehensive view of application behavior and resource consumption.

The second layer consists of the Cost-Aware Feature Engineering Module. Unlike traditional intrusion detection systems that focus exclusively on technical indicators, this module generates financial intelligence features directly associated with economic attack behavior. Examples include invocation cost estimates, cost growth rates, resource-to-cost conversion ratios, billing acceleration indices, cumulative expenditure trends, and budget utilization metrics. These features provide a direct representation of attack impact and allow the framework to identify malicious behaviors that may otherwise remain hidden within conventional telemetry data.

The third layer incorporates a Multi-Scale Analytics Engine responsible for extracting both temporal and frequency-domain information. The temporal branch utilizes deep sequential learning architectures to capture invocation dependencies, workload evolution patterns, and long-term behavioral trends. Simultaneously, the wavelet branch performs multi-resolution decomposition of cost-related signals to identify hidden anomalies occurring across different temporal scales. The integration of temporal and wavelet representations enables comprehensive characterization of both abrupt attack bursts and gradual cost escalation strategies.

A feature fusion mechanism subsequently combines outputs generated by both analytical branches. Through learned feature interactions, the system constructs a unified representation of serverless behavior that incorporates operational, temporal, frequency-domain, and economic characteristics. This integrated representation is then processed by an intelligent classification engine responsible for distinguishing normal activity from potential DoW attacks.

To improve operational trustworthiness, the framework includes an Explainable Security Intelligence Layer. This component provides interpretable insights into model decisions through feature attribution analysis, importance ranking, and visual explanation mechanisms. By identifying the factors responsible for attack predictions, the framework enables security analysts to understand why alerts are generated and supports informed decision-making during incident response operations.

The final layer consists of an Adaptive Defense and Mitigation Engine. Once malicious activity is detected, the framework automatically initiates appropriate countermeasures according to the estimated threat severity. Potential responses include invocation throttling, dynamic rate limiting, temporary function isolation, resource allocation control, adaptive scaling restrictions, budget protection policies, and automated administrator notifications. The objective is not merely to detect attacks but also to minimize financial impact through timely intervention.

The proposed framework offers several advantages over existing approaches. First, it explicitly integrates economic intelligence into the security analysis process. Second, it simultaneously exploits temporal and frequency-domain characteristics through multi-scale analytics. Third, it incorporates explainability mechanisms that improve operational transparency. Fourth, it supports real-time deployment through continuous monitoring and automated response capabilities. Finally, the framework establishes a foundation for future research into intelligent financial cybersecurity systems for cloud-native environments.

By combining cost-aware analytics, deep learning, wavelet-based signal processing, explainable artificial intelligence, and adaptive defense mechanisms, the proposed framework represents a comprehensive strategy for addressing the emerging challenge of Denial-of-Wallet attacks in serverless architectures.

V. Comparative Analysis of Existing DoW Detection Techniques

The growing threat of Denial-of-Wallet attacks has stimulated extensive research into intelligent detection and mitigation mechanisms for serverless environments. Existing approaches differ significantly in terms of analytical methodology, deployment complexity, computational overhead, detection capability, and economic awareness. Consequently, a systematic comparative evaluation is necessary to understand their relative strengths and limitations and to identify opportunities for future improvement.

Early defense mechanisms primarily relied on rule-based monitoring frameworks that utilized predefined thresholds associated with invocation frequency, execution duration, resource consumption, and billing expenditure. These approaches were attractive because of their simplicity and ease of deployment. Cloud service providers introduced native monitoring services capable of generating alerts whenever predefined spending limits or invocation thresholds were exceeded. Although these solutions offered low computational overhead and real-time response capabilities, their effectiveness remained limited against sophisticated adversaries capable of distributing malicious requests across multiple functions and time intervals. Furthermore, static thresholds often produced high false-positive rates under dynamic workload conditions, reducing their operational reliability.

To overcome these limitations, researchers introduced statistical anomaly detection techniques that model normal behavioral distributions and identify deviations from expected patterns. Approaches based on moving averages, Z-score analysis, Mahalanobis distance, clustering methods, and Isolation Forest algorithms demonstrated improved adaptability compared with threshold-based systems. Statistical models proved particularly effective for identifying abrupt deviations in invocation behavior and resource utilization. However, they frequently struggled to capture long-term temporal dependencies and evolving attack strategies, especially in large-scale serverless deployments characterized by highly variable workloads.

Machine learning approaches represented the next stage of development and introduced data-driven classification capabilities into DoW detection. Supervised learning algorithms such as Support Vector Machines, Random Forests, Gradient Boosting Machines, and Decision Trees demonstrated improved classification performance when trained on labeled attack datasets. These models successfully learned discriminative patterns associated with malicious behavior and reduced dependence on manually defined thresholds. Nevertheless, their performance remained strongly dependent on feature engineering quality. Most machine learning frameworks also treated observations as independent events, limiting their ability to capture sequential attack characteristics and temporal relationships inherent in serverless workloads.

Recent advances have increasingly focused on deep learning architectures due to their ability to automatically learn hierarchical feature representations from complex telemetry data. Convolutional Neural Networks have been employed to identify local patterns within invocation sequences, while recurrent architectures such as Long Short-Term Memory networks and Gated Recurrent Units have demonstrated strong capabilities in modeling temporal dependencies. Hybrid CNN-LSTM and CNN-GRU architectures have consistently outperformed conventional machine learning methods by simultaneously extracting spatial and temporal features. These systems achieve superior detection accuracy but often require significant computational resources and large training datasets.

Transformer-based architectures have emerged as another promising research direction because of their self-attention mechanisms and ability to model long-range dependencies. Several studies report impressive performance improvements using transformer-based intrusion detection frameworks. However, the computational complexity associated with attention operations presents challenges for real-time deployment in resource-constrained environments. Consequently, practical deployment of transformer-based security systems remains an active research challenge.

Wavelet-based detection frameworks have introduced a fundamentally different analytical perspective by examining serverless telemetry within both time and frequency domains. These approaches exploit the ability of wavelet transforms to decompose signals into multiple temporal scales, allowing simultaneous identification of sudden invocation bursts and long-term behavioral trends. Deep Wavelet Neural Networks further enhance this capability by integrating wavelet decomposition with neural learning mechanisms. Existing studies indicate that wavelet-based systems can identify subtle attack signatures that may remain undetected using purely temporal approaches. Nevertheless, most current implementations lack explicit economic-awareness mechanisms despite targeting financially motivated attacks.

Another important observation emerging from the literature is the limited integration of cloud financial indicators into detection frameworks. Most existing solutions primarily analyze technical metrics such as CPU utilization, memory consumption, network throughput, and invocation frequency. While these variables provide valuable operational insights, they do not directly represent the economic consequences that distinguish DoW attacks from traditional cybersecurity threats. As a result, many detection systems identify anomalies only after substantial financial damage has already occurred. This limitation has motivated increasing interest in cost-aware analytics and FinOps-oriented security frameworks.

A comprehensive review of the literature reveals that no existing solution simultaneously achieves high detection accuracy, economic awareness, explainability, deployment scalability, and real-time adaptability. Rule-based systems offer simplicity but lack intelligence. Statistical models improve adaptability but provide limited contextual understanding. Machine learning techniques enhance classification performance but often depend heavily on handcrafted features. Deep learning frameworks achieve superior accuracy but may suffer from computational complexity and reduced interpretability. Wavelet-based approaches capture

multi-scale patterns effectively but frequently overlook operational deployment requirements. These observations collectively justify the need for an integrated framework capable of combining the strengths of multiple analytical paradigms while addressing their individual weaknesses.

VI. Research Challenges and Open Issues

Despite significant progress in serverless security research, numerous challenges continue to hinder the development of robust and practical Denial-of-Wallet defense systems. These challenges span technical, operational, economic, and methodological dimensions, highlighting the complexity of protecting modern serverless infrastructures.

One of the most significant challenges involves the scarcity of publicly available datasets specifically designed for DoW attack research. Unlike traditional intrusion detection domains that benefit from numerous benchmark datasets, serverless security remains relatively immature. Existing datasets are often generated using simulated environments, making it difficult to assess how well detection models generalize to real-world cloud deployments. The absence of standardized benchmarking frameworks further complicates objective comparison among competing approaches.

Another critical issue concerns the dynamic and highly heterogeneous nature of serverless workloads. Invocation patterns vary significantly across applications, industries, and deployment environments. Functions supporting e-commerce platforms, IoT systems, healthcare applications, and financial services exhibit fundamentally different behavioral characteristics. Consequently, detection models trained on one workload distribution may experience substantial performance degradation when applied to another environment. Developing adaptive models capable of maintaining robustness across diverse operational conditions remains a major research challenge.

Data leakage represents another persistent methodological concern. Many published studies employ random train-test splitting strategies that inadvertently introduce temporal dependencies between training and evaluation datasets. Such practices can produce unrealistically high performance metrics that fail to reflect actual deployment conditions. Establishing rigorous experimental protocols, including chronological splitting, leakage auditing, and reproducibility validation, remains essential for advancing scientific rigor within this research domain.

The interpretability of artificial intelligence models also remains an unresolved challenge. While deep learning architectures frequently achieve superior predictive performance, they often function as black-box systems that provide limited explanation for their decisions. Security analysts and cloud administrators typically require transparent reasoning before initiating mitigation actions that may affect operational workloads. Consequently, integrating explainable artificial intelligence techniques into DoW detection frameworks represents an important research priority.

Real-time deployment constraints introduce additional complexity. Serverless environments generate large volumes of telemetry data that must be processed continuously with minimal latency. Detection systems must therefore balance analytical sophistication with computational efficiency. Excessively complex models may achieve high accuracy but fail to meet real-time operational requirements. Conversely, lightweight models may sacrifice predictive performance for computational efficiency. Achieving an optimal balance between these competing objectives remains challenging.

Economic intelligence represents another underexplored area. Although DoW attacks fundamentally target financial resources, most existing detection frameworks continue to focus predominantly on technical indicators. Developing security models that directly incorporate cloud expenditure metrics, cost escalation patterns, billing dynamics, and budget utilization behaviors represents a promising but largely unexplored research direction.

Finally, the increasing adoption of multi-cloud and hybrid-cloud architectures introduces additional security complexities. Organizations frequently deploy serverless applications across multiple cloud providers, each utilizing different billing models, monitoring frameworks, and execution environments.

Developing provider-agnostic defense mechanisms capable of operating consistently across heterogeneous infrastructures remains a significant open challenge for future research.

VII. Conclusion

Serverless computing has fundamentally transformed modern cloud application development by offering unprecedented scalability, flexibility, and cost efficiency. However, the same characteristics that make serverless architectures attractive also create opportunities for economically motivated cyberattacks. Among these threats, Denial-of-Wallet attacks have emerged as a particularly significant concern because they exploit cloud billing mechanisms rather than targeting service availability directly.

This review has comprehensively examined the current state of research on DoW attack detection and defense within serverless environments. The analysis demonstrated that existing approaches span a broad spectrum of methodologies, including rule-based monitoring systems, statistical anomaly detection techniques, machine learning algorithms, deep learning frameworks, and wavelet-based analytical models. While each category offers unique advantages, none independently provides a complete solution capable of addressing the technical, economic, operational, and explainability requirements of modern cloud security.

The comparative assessment identified several persistent challenges, including dataset scarcity, workload heterogeneity, methodological inconsistencies, limited interpretability, real-time deployment constraints, and insufficient integration of financial intelligence. These limitations indicate that current research remains in an evolutionary stage and that significant opportunities exist for innovation and advancement.

To address these challenges, this review proposed an Intelligent Cost-Aware Multi-Scale Defense Framework that integrates telemetry analytics, economic intelligence, deep learning, wavelet-based signal processing, explainable artificial intelligence, and adaptive mitigation strategies. The proposed framework establishes a conceptual foundation for future research aimed at developing resilient and economically aware cybersecurity systems for cloud-native infrastructures.

As serverless adoption continues to expand across critical application domains, the importance of cost-aware security analytics will increase correspondingly. Future advances in explainable artificial intelligence, federated learning, graph neural networks, digital twin technologies, and autonomous defense systems are expected to play a transformative role in shaping next-generation DoW detection frameworks. Ultimately, the convergence of cybersecurity intelligence and cloud financial analytics will be essential for ensuring the sustainability, resilience, and trustworthiness of future serverless computing ecosystems.

References

[1] P. Renukadevi, S. Amaran, A. Vikram, T. Prabhakara Rao, and M. K. Ishak, "Enhancing Cybersecurity Through Fusion of Optimization with Deep Wavelet Neural Networks on Denial of Wallet Attack Detection in Serverless Computing," IEEE Access, vol. 13, DOI: 10.1109/ACCESS.2025.3550735, 2025. [Base Paper]

[2] J. M. O. Candel, F. J. M. Gimeno, and H. M. Mora, "Generation of a Dataset for DoW Attack Detection in Serverless Architectures," Data in Brief, vol. 52, p. 109921, 2024. [Reference Paper]

[3] Y. Li, Y. Chen, and L. Wang, "A Comprehensive Survey on Serverless Computing Security: Threats, Countermeasures, and Future Directions," IEEE Access, vol. 9, pp. 56432–56451, 2021.

[4] C. Kelly, N. Zhang, and R. Schatz, "Denial-of-Wallet Attacks on Serverless Computing Platforms," in Proc. IEEE International Conference on Cloud Computing (CLOUD), pp. 234–243, 2021.

[5] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.

[6] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in Proc. IEEE International Conference on Data Mining (ICDM), pp. 413–422, 2008.

[7] K. Cho et al., "Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation," in Proc. EMNLP, pp. 1724–1734, 2014.

[8] J. Kim et al., "Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection," in Proc. International Conference on Platform Technology and Service (PlatCon), pp. 1–5, 2019.

[9] P. Barford, J. Kline, D. Plonka, and A. Ron, "A Signal Analysis of Network Traffic Anomalies," in Proc. ACM SIGCOMM Workshop on Internet Measurement (IMW), pp. 71–82, 2002.
[10] L. Li and G. Lee, "DDoS Attack Detection and Wavelets," Telecommunication Systems, vol. 28, no. 3, pp. 435–451, 2005.
[11] S. Miskhat, A. Rahman, and M. Islam, "Cost-Aware Anomaly Detection for Cloud Services: A Comprehensive Approach," Journal of Cloud Computing, vol. 12, no. 1, pp. 1–18, 2023.
[12] T. Lin, P. Goyal, R. Girshick, K. He, and P. Dollar, "Focal Loss for Dense Object Detection," in Proc. IEEE ICCV, pp. 2980–2988, 2017.
[13] I. Daubechies, "Ten Lectures on Wavelets," SIAM: Society for Industrial and Applied Mathematics, 1992.
[14] S. Mallat, "A Theory for Multiresolution Signal Decomposition: The Wavelet Representation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 11, no. 7, pp. 674–693, 1989.
[15] A. Paszke et al., "PyTorch: An Imperative Style, High-Performance Deep Learning Library," in Advances in NeurIPS, vol. 32, 2019.
[16] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.
[17] G. R. Lee et al., "PyWavelets: A Python Package for Wavelet Analysis," Journal of Open Source Software, vol. 4, no. 36, p. 1237, 2019.
[18] D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," in Proc. ICLR, 2015.
[19] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.
[20] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, pp. 436–444, 2015.
[21] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.
[22] A. Shahid, M. Faheem, and A. Maqsood, "Serverless Computing: A Survey of Opportunities, Challenges, and Applications," IEEE Access, vol. 10, pp. 63546–63564, 2022.
[23] D. Kelly, F. G. Glavin, and E. Barrett, "DoWNet—Classification of Denial-of-Wallet Attacks on Serverless Application Traffic," Journal of Cybersecurity, vol. 10, no. 1, p. tyae004, 2024.
[24] J. Shen, H. Zhang, Y. Geng, J. Li, J. Wang, and M. Xu, "Gringotts: Fast and Accurate Internal Denial-of-Wallet Detection for Serverless Computing," in Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 2627–2641, 2022.
[25] D. Kelly, F. G. Glavin, and E. Barrett, "Denial of Wallet—Defining a Looming Threat to Serverless Computing," Journal of Information Security and Applications, vol. 60, p. 102843, 2021.
[26] Z. Shuai, G. Yunfei, H. Hongchao, L. Wenyan, and W. Yawen, "ATSSC: An Attack Tolerant System in Serverless Computing," China Communications, vol. 21, no. 6, pp. 192–205, 2024.
[27] J. Xiong, M. Wei, Z. Lu, and Y. Liu, "Warmonger Attack: A Novel Attack Vector in Serverless Computing," IEEE/ACM Transactions on Networking, 2024.
[28] M. Akter, N. Moustafa, and B. Turnbull, "SPEI-FL: Serverless Privacy Edge Intelligence-Enabled Federated Learning in Smart Healthcare Systems," Cognitive Computation, pp. 1–16, 2024.
[29] P. Escaleira, V. A. Cunha, J. P. Barraca, D. Gomes, and R. L. Aguiar, "MoFaaS: A Moving Target Defense Approach to Fortify Functions as a Service," in Proc. IEEE Symposium on Computers and Communications (ISCC), pp. 1–7, 2024.
[30] C. Joshi, R. Deshmukh, H. Kalunge, S. Marathe, N. Ranjan, and P. K. Bhoyar, "High-Fidelity Simulated Dataset for Enhanced Detection of Denial of Wallet Attacks (DOW) in Serverless Architecture," in Proc. IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp. 1–6, 2024.
[31] 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.
[32] R. Soleymanzadeh, M. Aljasim, M. W. Qadeer, and R. Kashef, "Cyberattack and Fraud Detection Using Ensemble Stacking," AI, vol. 3, no. 1, pp. 22–36, 2022.
[33] F. Ullah, S. Ullah, G. Srivastava, and J. C.-W. Lin, "IDS-INT: Intrusion Detection System Using Transformer-Based Transfer Learning for Imbalanced Network Traffic," Digital Communications and Networks, vol. 10, no. 1, pp. 190–204, 2024.
[34] J. Guo, G. Zhou, K. Yan, Y. Sato, and Y. Di, "Pair Barracuda Swarm Optimization Algorithm: A Natural-Inspired Metaheuristic Method for High Dimensional Optimization Problems," Scientific Reports, vol. 13, no. 1, p. 18314, 2023.

[35] J. Zhang and Y. Diao, "Hierarchical Learning-Enhanced Chaotic Crayfish Optimization Algorithm: Improving Extreme Learning Machine Diagnostics in Breast Cancer," Mathematics, vol. 12, no. 17, p. 2641, 2024.
[36] C. A. Ananth and N. Krishnaraj, "Detection of Intrusions in Clustered Vehicle Networks Using Invasive Weed Optimization Using a Deep Wavelet Neural Networks," Measurement: Sensors, vol. 28, p. 100807, 2023.
[37] Y. Bengio, A. Courville, and P. Vincent, "Representation Learning: A Review and New Perspectives," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp. 1798–1828, 2013.
[38] M. Abadi et al., "TensorFlow: A System for Large-Scale Machine Learning," in Proc. USENIX Symposium on Operating Systems Design and Implementation (OSDI), pp. 265–283, 2016.
[39] P. Singh, M. Masud, M. S. Hossain, A. Kaur, G. Muhammad, and A. Ghoneim, "Privacy-Preserving Serverless Computing Using Federated Learning for Smart Grids," IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7843–7852, 2021.
[40] I. Polinsky, P. Datta, A. Bates, and W. Enck, "GRASP: Hardening Serverless Applications Through Graph Reachability Analysis of Security Policies," in Proc. ACM Web Conference (WWW), pp. 1644–1655, 2024.
[41] A. Vaswani et al., "Attention Is All You Need," in Advances in Neural Information Processing Systems (NeurIPS), vol. 30, 2017.
[42] M. A. I. Mallick and R. Nath, "Securing the Server-less Frontier: Challenges and Innovative Solutions in Network Security for Serverless Computing," Reading Time, pp. 04–15, 2024.
[43] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," in Proc. Military Communications and Information Systems Conference (MilCIS), pp. 1–6, 2015.
[44] M. V. Mahoney and P. K. Chan, "An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection," in Proc. International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 220–237, 2003.
[45] Z. Wang, "The Applications of Deep Learning on Traffic Identification," BlackHat USA Technical Report, 2015.
[46] A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761–768, 2018.
[47] S. Mudrakarta, A. Taly, M. Sundararajan, and K. Dhamdhere, "Did the Model Understand the Question?" in Proc. Annual Meeting of the Association for Computational Linguistics (ACL), pp. 1896–1906, 2018.
[48] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.
[49] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," in Proc. International Conference on Platform Technology and Service (PlatCon), pp. 1–5, 2016.
[50] Amazon Web Services, "AWS Lambda Security and Usage Patterns," AWS Documentation, 2024. [Online]. Available: https://docs.aws.amazon.com/lambda/latest/dg/security.html
[51] E. Jonas, J. Schleier-Smith, V. Sreekanti, C. Tsai, A. Khandelwal, Q. Pu, V. Shankar, J. Carreira, N. Krause, S. Lloyd, et al., "Cloud Programming Simplified: A Berkeley View on Serverless Computing," arXiv preprint arXiv:1902.03383, 2019.
[52] E. van Eyk, A. Iosup, S. Seif, and M. Thömmes, "The SPEC-RG Reference Architecture for FaaS and Serverless Computing," IEEE Internet Computing, vol. 22, no. 5, pp. 84–88, 2018.
[53] S. Hendrickson, S. Sturdevant, T. Harter, V. Venkataramani, A. C. Arpaci-Dusseau, and R. H. Arpaci-Dusseau, "Serverless Computation with OpenLambda," in Proc. USENIX HotCloud, pp. 33–39, 2016.
[54] G. McGrath and P. Brenner, "Serverless Computing: Design, Implementation, and Performance," in Proc. IEEE International Conference on Distributed Computing Systems Workshops, pp. 405–410, 2017.
[55] A. Baldini et al., "Serverless Computing: Current Trends and Open Problems," in Research Advances in Cloud Computing, Springer, pp. 1–20, 2017.
[56] E. Shahrad, J. Balkind, and D. Wentzlaff, "Architectural Implications of Function-as-a-Service Computing," in Proc. ACM/IEEE International Symposium on Computer Architecture (ISCA), pp. 1063–1075, 2019.

[57] M. Gusev and S. Dustdar, "Going Back to the Roots—The Evolution of Edge Computing, An IoT Perspective," IEEE Internet Computing, vol. 22, no. 2, pp. 5–15, 2018.
[58] G. Zhang, W. Li, M. A. Ferrag, and L. Shu, "Artificial Intelligence for Cloud Security: A Survey," IEEE Access, vol. 10, pp. 94712–94743, 2022.
[59] M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and T. Shu, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020.
[60] M. Alazab and R. Vinayakumar, "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 8, pp. 174306–174328, 2020.
[61] S. Lundberg and S. Lee, "A Unified Approach to Interpreting Model Predictions," in Proc. Advances in Neural Information Processing Systems (NeurIPS), vol. 30, 2017.
[62] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You? Explaining the Predictions of Any Classifier," in Proc. ACM SIGKDD, pp. 1135–1144, 2016.
[63] A. Taly, M. Sundararajan, and Q. Yan, "Integrated Gradients: Axiomatic Attribution for Deep Networks," in Proc. ICML, pp. 3319–3328, 2017.
[64] F. Hohman, M. Kahng, R. Pienta, and D. H. Chau, "Visual Analytics in Deep Learning: An Interrogative Survey for the Next Frontiers," IEEE Transactions on Visualization and Computer Graphics, vol. 25, no. 8, pp. 2674–2693, 2019.
[65] B. Settles, "Active Learning Literature Survey," University of Wisconsin–Madison Technical Report, 2010.
[66] Y. Kwon, S. Lee, and H. Kim, "Cost-Aware Resource Management in Cloud Computing: A Survey," Future Generation Computer Systems, vol. 124, pp. 95–112, 2021.
[67] A. Verma, G. Das, and K. Kant, "Cloud Cost Optimization and FinOps: Emerging Research Directions," IEEE Cloud Computing, vol. 11, no. 1, pp. 22–34, 2024.
[68] J. Spillner and S. Dorodko, "Economic Security Challenges in Serverless Cloud Computing," Future Internet, vol. 14, no. 3, p. 85, 2022.
[69] M. Ahmed, A. Naser Mahmood, and J. Hu, "A Survey of Network Anomaly Detection Techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.
[70] H. Ringberg, A. Soule, J. Rexford, and C. Diot, "Sensitivity of PCA for Traffic Anomaly Detection," ACM SIGMETRICS Performance Evaluation Review, vol. 35, no. 1, pp. 109–120, 2007.
[71] D. Brauckhoff, X. Dimitropoulos, A. Wagner, and K. Salamatian, "Anomaly Extraction in Backbone Networks Using Association Rules," IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1788–1799, 2012.
[72] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A Taxonomy of Network Threats and Intrusion Detection Systems," Future Internet, vol. 12, no. 1, p. 7, 2020.
[73] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the Development of Realistic Botnet Dataset in the Internet of Things," Information Sciences, vol. 557, pp. 229–251, 2021.
[74] M. A. Ferrag, M. Babaghayou, and M. Yazici, "Cyber Security for Cloud Computing: A Review of Recent Advances," Computer Communications, vol. 190, pp. 141–168, 2022.
[75] A. A. Diro, N. Chilamkurti, and S. Nam, "Deep Learning-Based Security Solutions for Distributed Systems," IEEE Transactions on Network Science and Engineering, vol. 9, no. 2, pp. 1040–1055, 2022.
[76] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes," IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 1, pp. 41–55, 2007.
[77] J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," Communications of the ACM, vol. 51, no. 1, pp. 107–113, 2008.
[78] L. Bottou, F. E. Curtis, and J. Nocedal, "Optimization Methods for Large-Scale Machine Learning," SIAM Review, vol. 60, no. 2, pp. 223–311, 2018.
[79] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proc. ACM SIGKDD, pp. 785–794, 2016.
[80] H. He and E. Garcia, "Learning from Imbalanced Data," IEEE Transactions on Knowledge and Data Engineering, vol. 21, no. 9, pp. 1263–1284, 2009.