Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

JOURNAL OF SCIENTIFIC LETTERS
www.jslsci.com

DESIGN AND DEVELOPMENT OF AN INTELLIGENT SERVERLESS ARCHITECTURE FOR ADVANCED THREAT DETECTION IN CLOUD COMPUTING ENVIRONMENTS

Bandi Madhusudhan

Research Scholar, Dept. of CSE, Sikkim Alpine University, Namchi Sikkim

Dr. Pankaj Khairnar

Research Supervisor, Dept. of CSE, Sikkim Alpine University, Namchi Sikkim

ABSTRACT

The rapid expansion of cloud computing has increased the complexity of cybersecurity threats, creating a need for intelligent and scalable security mechanisms. Traditional threat detection systems often encounter limitations in processing dynamic workloads, identifying sophisticated attacks, and responding to emerging vulnerabilities. Serverless computing offers an innovative approach by providing event-driven execution, automatic scalability, and reduced infrastructure management requirements. This research proposes an intelligent serverless architecture designed to strengthen threat detection capabilities in cloud computing environments. The proposed framework integrates machine learning, real-time event monitoring, behavioural analysis, and automated security responses to identify suspicious activities. It focuses on detecting unauthorized access, malicious code execution, abnormal resource consumption, and network-based attacks. The architecture aims to improve detection efficiency, operational flexibility, and resource utilization while reducing security management overhead.

Keywords: Serverless Computing, Cloud Security, Threat Detection, Machine Learning, Intelligent Architecture, Cybersecurity, Anomaly Detection.

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

I. INTRODUCTION

Cloud computing has transformed the modern technological environment by providing flexible, scalable, and cost-effective computing resources. Organizations increasingly depend on cloud-based platforms to manage applications, store confidential information, and perform complex computational activities. However, the growing adoption of cloud infrastructure has also expanded the possibilities for cyberattacks, unauthorized access, data manipulation, and malicious activities. Traditional security mechanisms frequently face difficulties in addressing these challenges because cloud environments involve distributed resources, interconnected services, dynamic workloads, and continuously changing application configurations. Consequently, advanced security approaches are necessary to protect cloud resources and maintain the confidentiality, integrity, and availability of information.

Serverless computing represents an emerging cloud service model in which infrastructure provisioning, server maintenance, and resource allocation are largely managed by cloud service providers. Developers can concentrate on application functionality through independently executed functions that respond to specific events. This architecture supports automatic scaling and reduces the operational responsibilities of organizations. Nevertheless, serverless environments introduce particular security challenges, including insecure function configurations, excessive permissions, vulnerable dependencies, event manipulation, and limited execution visibility. Marin, Perino, and Di Pietro (2022) explain that the architectural characteristics of serverless computing create security concerns requiring specialized protection mechanisms rather than relying exclusively on conventional cloud security solutions.

Intelligent threat detection has become an important component of modern cybersecurity because conventional signature-based mechanisms cannot always recognize previously unidentified or rapidly changing attacks. Machine learning and behavioural analytics provide opportunities to examine execution patterns, identify unusual activities, and classify potentially malicious events. By analyzing function invocation frequency, authentication records, network requests, resource utilization, and access permissions, intelligent systems can recognize deviations from established operational patterns. Integrating these capabilities into serverless environments can provide a flexible mechanism for continuous monitoring and rapid security assessment.

The present research proposes the design and development of an intelligent serverless architecture for advanced threat detection in cloud computing environments. The proposed framework

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

combines event-driven monitoring, machine-learning-based anomaly identification, centralized security intelligence, and automated response mechanisms. Its primary objective is to develop a security-oriented architecture capable of identifying suspicious activities without creating unnecessary infrastructure complexity. The research also considers architectural flexibility, detection accuracy, execution efficiency, and resource optimization as important evaluation dimensions. The proposed model provides a conceptual foundation for developing adaptive cloud security systems that can respond effectively to changing cybersecurity requirements.

II. INTELLIGENT SERVERLESS ARCHITECTURE AND ITS CORE COMPONENTS

The proposed intelligent serverless architecture is designed to integrate security monitoring and threat identification directly into cloud-based application workflows. Unlike conventional security systems that depend heavily on continuously running monitoring servers, the proposed framework uses event-triggered functions to perform specific security operations whenever relevant activities occur. These activities may include application requests, authentication attempts, database modifications, changes in access permissions, and unusual network communications. The event-driven approach enables security processes to operate according to actual workload requirements, supporting flexibility and efficient resource utilization.

The first component of the architecture is the event collection and monitoring layer. This layer receives information from cloud applications, application programming interfaces, identity management services, databases, and network gateways. Every relevant activity generates an event containing information about the source, timestamp, requested operation, user identity, and associated resources. The collected information is forwarded to serverless monitoring functions for preliminary examination. Appropriate event normalization is essential because different cloud services may generate information in different formats. Standardized event records facilitate consistent analysis and improve the ability to correlate activities across multiple cloud services.

The second component involves intelligent data processing and feature extraction. Raw security events frequently contain unnecessary information, repeated records, and inconsistent attributes. Therefore, preprocessing functions are employed to remove redundant information, normalize event values, and extract meaningful security indicators. Important indicators may include login frequency, failed authentication attempts, unusual geographic access patterns, function execution duration, request volume, privilege changes, and unexpected data transfers. These characteristics

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

provide the foundation for identifying deviations from normal system behaviour. The architecture can also maintain historical behavioural profiles to support more informed security decisions.

The third component is the machine-learning-based threat detection engine. This component examines processed event information and identifies activities that demonstrate suspicious characteristics. Supervised learning algorithms can classify known attack patterns, while unsupervised techniques can identify unusual behaviour without requiring previously labelled attack examples. Algorithms such as decision trees, random forests, clustering, and neural networks may be considered according to the nature of the available data. The detection engine produces a threat score that represents the estimated severity of an identified activity. This score supports the classification of events into normal, suspicious, and potentially malicious categories.

The fourth component is the security orchestration and response layer. Once suspicious behaviour is detected, the architecture activates appropriate serverless response functions. Depending on the identified threat, these functions may temporarily restrict access, revoke compromised credentials, isolate affected application components, block suspicious requests, or notify security administrators. Automated responses should follow predefined policies and authorization requirements to avoid unnecessary service disruption. Critical actions, particularly those affecting sensitive applications or business operations, may require human approval. This combination of automated processing and controlled administrative intervention strengthens operational reliability.

The final component involves secure storage, reporting, and continuous improvement. Detection results, security alerts, incident records, and response activities are maintained through protected logging and monitoring services. These records provide an audit trail for investigating security incidents and evaluating system performance. Feedback from confirmed incidents can also support periodic model refinement and policy improvement. The architecture should incorporate encryption, access restrictions, retention policies, and integrity verification to protect collected security information. Through these interconnected components, the proposed framework establishes an adaptable foundation for intelligent threat detection in serverless cloud environments.

III. MACHINE LEARNING-BASED THREAT IDENTIFICATION AND BEHAVIOURAL ANALYSIS

Machine learning provides an important foundation for developing intelligent cybersecurity

systems because it enables automated examination of large volumes of operational information. In cloud computing environments, security events are generated continuously through application requests, authentication activities, database transactions, and interactions between distributed services. Manual examination of every event is impractical, particularly when applications experience sudden increases in workload. Machine-learning-based analysis can process these records and identify relationships that may indicate suspicious activities. Integrating these techniques with serverless functions enables security analysis to be performed dynamically whenever relevant events are generated.

Behavioural analysis is particularly important because malicious activities do not always match previously identified attack signatures. An attacker may use legitimate credentials, exploit application permissions, or generate requests that appear normal when examined individually. However, a sequence of unusual activities may indicate an attempt to compromise the cloud environment. The proposed architecture establishes behavioural baselines using historical information about users, applications, and serverless functions. Deviations from these baselines are examined through predefined thresholds and machine-learning models. For example, repeated authentication failures followed by an unusual administrative request may indicate credential abuse or unauthorized privilege escalation.

Supervised learning can be used to classify known security threats when sufficiently representative labelled datasets are available. Random forest and decision-tree algorithms can examine combinations of behavioural characteristics and identify patterns associated with suspicious activities. These models may classify events into categories such as unauthorized access, abnormal resource consumption, suspicious function invocation, and potential data exfiltration. However, the reliability of supervised classification depends on the quality, diversity, and representativeness of training information. Inadequate datasets may produce inaccurate predictions, particularly when the cloud environment encounters previously unseen attack techniques.

Unsupervised learning provides an additional mechanism for identifying unfamiliar patterns. Clustering and isolation-based approaches can examine event characteristics and identify observations that differ significantly from established behavioural groups. Such methods are useful when labelled security information is limited. Nevertheless, unusual activity does not necessarily represent a cyberattack. Legitimate operational changes, application updates, and unexpected workload increases may also generate anomalies. Therefore, the proposed framework

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

combines anomaly scores with contextual information, access policies, and historical activity records to reduce unnecessary security alerts.

Threat prioritization is another essential feature of the proposed detection mechanism. Not every suspicious event presents an equivalent level of risk. An unsuccessful login attempt may represent a relatively limited concern, whereas unauthorized access to sensitive databases or administrative resources may require immediate intervention. The architecture calculates threat severity using multiple indicators, including event frequency, resource sensitivity, privilege level, behavioural deviation, and potential operational impact. These indicators can be combined into a risk-scoring mechanism that helps security administrators distinguish between low-, medium-, and high-priority incidents.

Continuous model evaluation is necessary to maintain the effectiveness of intelligent threat identification. Cloud applications evolve over time, and changes in user behaviour, software configurations, and workload characteristics can influence detection performance. Periodic evaluation should therefore examine precision, recall, F1-score, false-positive rate, false-negative rate, and processing latency. Model updates should be validated before deployment to avoid introducing inaccurate classifications. Explainability mechanisms should also provide understandable reasons for important alerts, helping administrators determine why particular events were classified as suspicious. In this manner, machine learning and behavioural analytics contribute to a more adaptive and transparent cloud security architecture.

IV. SECURITY IMPLEMENTATION, PERFORMANCE OPTIMIZATION AND EVALUATION

The successful implementation of an intelligent serverless security architecture requires careful consideration of application design, cloud configuration, data protection, and operational policies. The proposed model can be implemented through cloud functions connected to event-management services, protected storage systems, identity management mechanisms, and centralized monitoring facilities. Individual security functions should perform clearly defined tasks, including event collection, preprocessing, anomaly detection, alert generation, and response execution. This modular structure allows individual components to be updated without requiring extensive modifications to the entire security system. It also supports integration with different cloud platforms and application environments.

Identity and access management represent essential implementation requirements. Serverless

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

functions frequently interact with storage services, databases, application interfaces, and other cloud resources. Excessive permissions may allow compromised functions to perform unauthorized operations. Therefore, the proposed architecture adopts the principle of least privilege, according to which each function receives only the permissions required to complete its assigned task. Credentials should be managed through secure identity services rather than embedded directly in application code. Authentication mechanisms, role-based access controls, and periodic permission reviews further strengthen the protection of sensitive cloud resources.

Data protection is equally important because security monitoring systems frequently process information containing user identifiers, network details, application records, and operational metadata. The proposed framework requires encryption during transmission and storage, appropriate data retention policies, and controlled access to monitoring records. Sensitive information should be minimized or anonymized wherever possible. Secure communication between event sources and analytical functions reduces the possibility of unauthorized information interception. In addition, audit records should be protected against unauthorized modification to preserve their usefulness during incident investigation and compliance assessments.

Performance optimization is necessary because security functions introduce additional processing requirements into cloud applications. Excessive monitoring may increase execution time, resource consumption, and operational costs. The proposed architecture addresses these concerns through selective event collection, lightweight preprocessing, asynchronous processing, and risk-based analysis. High-priority security events can be examined immediately, while less critical records may be processed through scheduled analytical functions. Caching frequently used information and reducing unnecessary data transfers may further improve execution efficiency. The system should also account for cold-start delays, concurrency restrictions, execution time limits, and provider-specific service limitations.

The evaluation of the proposed architecture should be conducted through a controlled experimental environment containing representative serverless applications and simulated security events. Relevant scenarios may include repeated authentication failures, unauthorized function invocation, abnormal request volumes, suspicious privilege modifications, and unexpected data access. The proposed system can be compared with conventional signature-based monitoring and rule-based detection approaches. Evaluation indicators should include detection accuracy, precision, recall, false-alarm frequency, response time, execution overhead, and operational cost. Such a comparison would help establish whether intelligent serverless monitoring offers practical

E-mail: editor.jslsci888@gmail.com

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

improvements under different workload conditions.

Finally, implementation should incorporate continuous auditing and incident-response validation. Security administrators should periodically examine detected incidents, verify automated response decisions, and update security policies according to changing operational requirements. Particular attention should be given to model drift, adversarial manipulation, event spoofing, and unauthorized access to monitoring components. The framework should also maintain recovery procedures for situations in which automated response functions become unavailable. These measures support the development of a dependable security environment in which threat detection, operational monitoring, and incident management work together to protect cloud-based applications.

V. CONCLUSION

The increasing dependence on cloud computing has created substantial requirements for advanced security mechanisms capable of identifying sophisticated cyber threats in dynamic and distributed environments. Conventional security approaches frequently face limitations when dealing with rapidly changing application workloads, distributed execution processes, and previously unidentified attack patterns. Serverless computing provides an opportunity to address certain operational challenges through event-driven execution, automatic resource allocation, and reduced infrastructure management. However, its distinctive architectural characteristics also require specialized security mechanisms to protect applications, functions, and associated cloud resources.

The proposed research presents an intelligent serverless architecture that integrates event monitoring, machine-learning-based threat identification, behavioural analysis, and automated security responses. The framework is designed to collect relevant security events, examine operational patterns, classify suspicious activities, and initiate appropriate protective actions. Its modular structure supports scalability and flexibility while allowing individual security components to operate according to workload requirements. The integration of supervised and unsupervised learning techniques offers opportunities to identify both recognized threats and unusual activities that may indicate emerging attacks.

The research also emphasizes the importance of secure implementation, identity management, encryption, performance optimization, and continuous evaluation. Detection accuracy alone

cannot determine the overall effectiveness of a cloud security system. Response latency, false-positive rates, execution overhead, resource utilization, and operational cost must also be considered. Furthermore, automated security decisions should remain transparent, auditable, and subject to appropriate administrative controls. These requirements are particularly important when security functions interact with sensitive business applications and confidential information.

Future research may focus on implementing the proposed architecture using commercial and open-source serverless platforms and evaluating its performance through realistic cyberattack scenarios. Advanced learning techniques, explainable artificial intelligence, federated analysis, and adaptive incident-response mechanisms may further strengthen its capabilities. Additional investigation is also required to examine resistance against adversarial attacks, model manipulation, and emerging vulnerabilities in function execution environments. Overall, the proposed architecture provides a conceptual foundation for developing intelligent, scalable, and adaptive threat dete ction mechanisms that can contribute to improved security and reliability in modern cloud computing environments.

REFERENCES

1. A & Achuthan, K 2022, ‘Threat Modeling and Threat Intelligence System for Cloud using Splunk,’ Proceedings of 10th International Symposium on Digital Forensics and Security (ISDFS), IEEE,2022, pp. 1-6.

2. Abbas, N, Zhang, Y, Taherkordi, A &Skeie, T 2017, ‘Mobile edge computing: A survey,’ IEEE Internet of Things Journal, vol. 5, issue no. 1, pp. 450–465.

3. Abdelrazek, Mohamed & Grundy, John & Mueller, Ingo. (2016). An Analysis of the Cloud Computing Security Problem. 10.48550/arXiv.1609.01107.

4. Abu, Md & Mallick, Md & Nath, Rishab. (2024). Securing the Server-less Frontier: Challenges and Innovative Solutions in Network Security for Server- less Computing. 193. 1-45.

5. Afzaliseresht, N, Miao, Y, Michalska, S, Liu, Q & Wang, H 2020, ‘From logs to Stories: Human-Centred Data Mining for Cyber Threat Intelligence,’ in IEEE Access, vol. 8, pp. 19089-19099.

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

6. Agarwal P &Alam, M 2020, 'A lightweight deep learning model for human activity recognition on edge devices,' Procedia Computer Science, vol.167, pp. 2364–2373.

7. Ahmadi, Sina. (2024). Challenges and Solutions in Network Security for Serverless Computing. International Journal of Current Science Research and Review. 7. 218-229. 10.47191/ijcsrr/V7-i1-23.

8. Ahmed, AA &Echi, M 2021, 'Hawk-eye: An ai-powered threat detector for intelligent surveillance cameras,' IEEE Access, vol. 9, pp. 63283– 63293.

9. Akshay, T, SibiChakkaravarthy, S, Sangeetha, D, VenkataRathnam, M &Vaidehi, V 2019, 'Role Based Policy to Maintain Privacy of Patient Health Records in Cloud', Journal of Super Computing, vol.75, no. 9, pp.5866–5881.

10. Al-Hawawreh, M, Moustafa, N, Garg, S & Hossain, MS 2021, 'Deep learning-enabled threat intelligence scheme in the internet of things networks,' IEEE Transactions on Network Science and Engineering, vol. 8, no. 4, pp. 2968–2981.