JOURNAL OF THE ROYAL LAUREATES ACADEMY

www.rlaindia.org

ENHANCING CLOUD SECURITY THROUGH SERVERLESS COMPUTING: A NOVEL APPROACH TO REAL-TIME CYBER THREAT IDENTIFICATION AND PREVENTION

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 increasing adoption of cloud computing has created new cybersecurity challenges involving unauthorized access, malicious network activities, data breaches, and sophisticated cyberattacks. Traditional security mechanisms frequently experience difficulties in providing immediate protection against continuously evolving threats. Serverless computing offers an effective architectural opportunity through event-driven processing, automatic scalability, and flexible resource allocation. This research examines a novel approach to enhancing cloud security through serverless computing by integrating real-time threat identification, intelligent monitoring, behavioural analytics, and automated prevention mechanisms. The proposed framework continuously evaluates cloud activities and activates security functions whenever potentially malicious events are detected. It emphasizes rapid threat classification, contextual risk assessment, and automated incident response to reduce security vulnerabilities. The study also considers operational efficiency, detection reliability, scalability, and data protection. The proposed approach provides a conceptual foundation for developing responsive and adaptive cybersecurity mechanisms for contemporary cloud computing environments.

Keywords: Cloud Security, Serverless Computing, Real-Time Threat Detection, Cyber Threat Prevention, Intrusion Detection, Automated Response, Cloud Infrastructure.

I. INTRODUCTION

The widespread adoption of cloud computing has fundamentally changed how organizations develop, deploy, and manage digital applications. Cloud platforms provide flexible infrastructure, remote accessibility, centralized storage, and on-demand computing resources. These characteristics support organizational efficiency and enable businesses to expand their technological operations without maintaining extensive physical infrastructure. However, the increasing dependence on interconnected cloud services has also created significant cybersecurity risks. Unauthorized access, ransomware, malicious software, distributed denial-of-service attacks, credential theft, and data manipulation represent important threats to cloud-based information systems. Consequently, organizations require security mechanisms capable of identifying suspicious activities and responding to potential attacks before they cause substantial damage.

Traditional cybersecurity systems generally depend on predefined security rules, signature databases, and centralized monitoring infrastructure. Although these approaches remain useful for recognizing established attack patterns, they may encounter difficulties when dealing with rapidly changing threats and distributed cloud workloads. Delays in identifying suspicious activities can allow attackers to exploit vulnerabilities, compromise sensitive information, and interrupt application services. Moreover, the continuously changing nature of cloud environments makes it difficult to maintain conventional security configurations across different applications and computing resources. Real-time monitoring and automated threat prevention have therefore become important requirements for strengthening cloud security.

Serverless computing introduces an event-driven execution model in which cloud service providers manage much of the underlying infrastructure. Applications are divided into functions that execute when specific events occur, enabling organizations to respond dynamically to changing workload requirements. This approach can also support security operations by activating monitoring and response functions whenever authentication attempts, application requests, network activities, or resource modifications are detected. Nevertheless, serverless environments introduce specific concerns involving function permissions, execution isolation, event validation, third-party dependencies, and limited visibility into infrastructure-level activities. Existing research emphasizes that these challenges require security mechanisms specifically designed for serverless architectures (Marin et al., 2022; Escaleira et al., 2025).

The present research examines a novel approach to enhancing cloud security through serverless computing by integrating continuous event monitoring, intelligent threat classification, and automated prevention mechanisms. The proposed framework aims to identify potentially malicious activities in real time and activate appropriate security responses according to their severity. It emphasizes rapid incident identification, contextual risk evaluation, secure function execution, and operational scalability. The study also considers the importance of reducing false alarms, minimizing response delays, and protecting confidential information. By combining serverless architecture with intelligent cybersecurity techniques, the proposed approach establishes a conceptual model for improving the responsiveness and reliability of cloud security systems.

II. REAL-TIME CYBER THREAT IDENTIFICATION THROUGH EVENT-DRIVEN SERVERLESS COMPUTING

Real-time threat identification is an essential requirement for protecting cloud computing environments against continuously evolving cyberattacks. Conventional monitoring systems may experience operational limitations when they depend on centralized processing mechanisms to examine large volumes of security information. Serverless computing provides an alternative approach through event-triggered functions that execute whenever relevant activities occur. These functions can monitor application requests, authentication events, database operations, network communications, and changes in cloud configurations. By processing security-related events as they are generated, organizations can establish a responsive monitoring mechanism that reduces dependence on continuously operating security servers.

The proposed framework begins with a real-time event acquisition mechanism that collects information from different cloud services. These sources may include application gateways, identity management systems, storage services, database platforms, and serverless execution environments. Every event is examined for important attributes such as source identity, timestamp, requested operation, resource destination, access privileges, and execution status. Standardization of event information is necessary because different cloud services may produce different logging formats. An event normalization mechanism converts these records into a consistent structure that can be processed by analytical functions. This improves the ability to identify relationships between activities occurring across different cloud components.

The next stage involves intelligent examination of incoming security information. Serverless analytical functions process event records and identify patterns that may indicate suspicious behaviour. These patterns may include repeated unsuccessful login attempts, unusual access to sensitive resources, unexpected changes in application permissions, and abnormal request volumes. Behavioural analytics can also compare current activities with previously established user and application profiles. For example, an application that normally generates a limited number of database requests may require additional investigation if its request frequency increases suddenly without an identifiable operational reason. Contextual examination helps distinguish suspicious behaviour from ordinary workload fluctuations.

Machine learning can further strengthen real-time threat identification by examining relationships among multiple security indicators. Supervised classification techniques can recognize previously documented attack patterns, while unsupervised anomaly detection can identify activities that differ significantly from normal operational behaviour. Random forests, decision trees, clustering algorithms, and isolation-based methods may be incorporated according to the available information and computational requirements. The detection engine assigns a risk score to suspicious events, allowing the system to prioritize activities according to their estimated severity. This approach helps security administrators concentrate on incidents that present the greatest potential danger to cloud resources.

Another important feature involves correlating related security events across multiple application components. Individual events may appear harmless when examined independently, but their combined occurrence can reveal a more serious security incident. For example, repeated login failures, an unexpected successful authentication, and subsequent access to confidential records may indicate a compromised account. The proposed architecture uses correlation functions to examine these activities within relevant time intervals and identify potentially connected incidents. Event correlation improves contextual understanding and reduces dependence on isolated security alerts. It also provides a stronger foundation for determining whether an unusual activity represents a genuine security concern.

The final identification stage involves generating structured security alerts and maintaining incident records. Alerts should include information about the detected activity, associated resources, estimated severity, relevant behavioural indicators, and recommended responses. Security administrators can use this information to investigate incidents and determine whether additional protective measures are necessary. The system should also maintain protected audit records to support future analysis and regulatory requirements. Through

continuous event collection, intelligent examination, and contextual correlation, the proposed serverless mechanism establishes a flexible approach to identifying cyber threats within dynamic cloud computing environments.

III. AUTOMATED THREAT PREVENTION AND ADAPTIVE SECURITY RESPONSE MECHANISMS

Identifying cyber threats is only one part of an effective cloud security strategy. Timely prevention and appropriate incident response are equally important because delayed intervention can allow attackers to compromise additional resources. The proposed framework integrates automated response mechanisms with serverless computing to initiate protective actions whenever suspicious activities exceed predefined risk thresholds. These actions may include restricting access, blocking suspicious requests, suspending compromised credentials, isolating affected functions, and notifying responsible security administrators. The event-driven architecture enables these protective functions to execute according to the characteristics and severity of detected incidents.

The automated response mechanism operates through a risk-based decision process. Every identified security event is evaluated according to its potential impact, the sensitivity of the affected resource, the level of access involved, and the confidence of the detection mechanism. Low-risk events may generate monitoring notifications, while medium-risk incidents may activate additional authentication requirements or temporary restrictions. High-risk incidents may require immediate access suspension, function isolation, or other protective actions. This classification prevents the system from applying identical responses to security incidents with different operational consequences. It also supports more efficient use of security resources.

Access control represents an important component of automated prevention. Many cloud security incidents occur because users, applications, or serverless functions possess permissions beyond those necessary for their responsibilities. The proposed framework adopts least-privilege access policies and continuously evaluates authorization-related activities. When suspicious permission changes are identified, the system can generate alerts and initiate appropriate corrective actions. Temporary credential revocation, access restriction, and additional identity verification may be used to reduce the possibility of unauthorized operations. These measures help limit the impact of compromised accounts and prevent unnecessary access to confidential cloud resources.

Adaptive response is another important feature because cyber threats frequently change their techniques to avoid conventional security controls. A fixed response mechanism may become ineffective when attackers modify their behaviour or exploit new vulnerabilities. The proposed architecture therefore incorporates contextual risk evaluation and feedback-based policy improvement. Historical incidents, confirmed alerts, and administrator decisions can be examined to refine response rules. However, automatic policy modification should be subject to validation and appropriate approval procedures. This is necessary to prevent inaccurate model decisions from creating additional security vulnerabilities or disrupting legitimate cloud applications.

The architecture also incorporates incident containment and recovery procedures. When a potentially compromised function or application component is detected, the system may restrict its access to sensitive services and preserve relevant execution records for investigation. Security administrators can subsequently examine the incident, identify its possible origin, and determine the extent of the compromise. Recovery procedures may involve credential replacement, software updates, configuration correction, and restoration of affected application components. Protected backups and verified deployment configurations are important for maintaining service continuity. The integration of detection, containment, investigation, and recovery creates a more comprehensive security response mechanism.

Human supervision remains necessary even when automated prevention functions are available. Security systems may incorrectly classify legitimate workload changes as malicious activities, particularly when application behaviour changes unexpectedly. Therefore, high-impact actions should be governed by clearly defined policies and, where appropriate, administrative approval. Explainable alerts should provide information about the indicators responsible for a particular security decision. Administrators should also be able to review response histories, modify security policies, and reverse inappropriate actions. This combination of intelligent automation and human oversight strengthens the reliability, transparency, and accountability of cloud security operations.

IV. PERFORMANCE OPTIMIZATION, SECURITY RELIABILITY AND PRACTICAL EVALUATION

The practical effectiveness of a serverless cloud security framework depends on its ability to provide reliable protection without introducing excessive computational overhead. Although serverless computing supports automatic scaling and event-driven execution, security

functions still require processing resources and may influence application performance. Frequent monitoring activities, large volumes of event records, and complex machine-learning operations can increase execution costs and response delays. Therefore, the proposed framework emphasizes lightweight processing, selective monitoring, asynchronous execution, and efficient resource allocation. These techniques help maintain a balance between security requirements and operational performance.

Scalability is an important advantage of serverless computing because security functions can respond dynamically to changing event volumes. During periods of increased application activity, additional function instances may be activated according to the capabilities and limitations of the selected cloud platform. This flexibility is particularly valuable for organizations operating applications with unpredictable workloads. However, concurrency limits, function execution time restrictions, cold-start delays, and event-processing bottlenecks must be considered during implementation. Proper configuration of event queues and processing limits can help manage sudden increases in security information and reduce the possibility of monitoring failures.

Security reliability requires the protection of both the monitored cloud environment and the security framework itself. Monitoring functions should operate with restricted permissions and communicate through authenticated channels. Event records should be protected through encryption and appropriate integrity controls. Sensitive credentials must be stored using secure secrets-management services rather than embedded in application code. Furthermore, access to security dashboards, incident records, and automated response functions should be limited to authorized personnel. These safeguards prevent attackers from manipulating monitoring information or disabling protective mechanisms after gaining access to the cloud environment.

Evaluation of the proposed framework should involve a controlled experimental environment containing representative cloud applications and simulated cyberattack scenarios. Relevant test cases may include brute-force authentication attempts, unauthorized API access, abnormal function invocation, suspicious database queries, and unexpected resource consumption. The framework can be compared with conventional rule-based monitoring and signature-based detection systems. Important evaluation indicators include detection accuracy, precision, recall, F1-score, false-positive rate, response latency, execution overhead, and operational cost. Such testing would help determine whether serverless security functions provide meaningful improvements in responsiveness and threat identification.

Operational reliability should also be examined under different workload conditions. Security mechanisms must continue to function when applications experience sudden increases in activity, communication failures, or temporary service interruptions. The proposed framework should therefore incorporate retry policies, event buffering, failure notifications, and recovery procedures. Duplicate event handling and inconsistent incident records should also be addressed to prevent inaccurate security decisions. Regular testing of automated response mechanisms is necessary to verify that protective actions operate as intended and do not unnecessarily interrupt legitimate services.

Finally, the practical implementation of the proposed approach should consider regulatory requirements, data privacy, auditability, and long-term maintenance. Organizations may need to preserve security records, document incident responses, and demonstrate appropriate access controls. Periodic model evaluation is also important because changing application workloads can reduce the reliability of previously established behavioural baselines. Continuous improvement should involve reviewing confirmed incidents, updating detection models, and validating revised response policies before deployment. Through these measures, serverless computing can support the development of an adaptive security framework that combines real-time threat identification, automated prevention, and efficient cloud resource management.

V. CONCLUSION

The growing adoption of cloud computing has increased the importance of developing security mechanisms that can identify and prevent cyber threats in rapidly changing digital environments. Conventional security approaches may experience difficulties when dealing with distributed applications, continuously generated event information, and sophisticated attack techniques. Serverless computing offers a flexible foundation for improving security operations through event-driven execution, automatic scaling, and modular processing. Nevertheless, its distinctive execution model requires specialized monitoring, access management, and threat prevention mechanisms to address potential vulnerabilities effectively.

The present research proposes a novel conceptual approach to enhancing cloud security through serverless computing by integrating real-time event monitoring, intelligent threat identification, behavioural analysis, and automated response mechanisms. The framework is designed to examine activities across cloud applications and identify suspicious patterns

through machine-learning-based classification and contextual risk assessment. Its automated prevention component supports protective actions such as access restriction, credential suspension, suspicious request blocking, and function isolation. These capabilities can contribute to reducing the time between threat identification and appropriate security intervention.

The study further emphasizes performance optimization, security reliability, data protection, and continuous evaluation as essential requirements for successful implementation. An effective cloud security architecture must provide reliable detection without creating unnecessary operational overhead or interrupting legitimate application activities. Therefore, evaluation should consider detection accuracy, false-positive rates, response time, scalability, execution costs, and resource utilization. Human supervision, explainable alerts, and secure audit records are also important for maintaining accountability and ensuring that automated security decisions remain appropriate.

Future research may concentrate on implementing the proposed framework through different serverless platforms and testing its effectiveness against realistic cyberattack scenarios. Advanced artificial intelligence, adaptive access control, federated learning, and automated incident recovery may provide additional opportunities to strengthen cloud protection. Further investigation is also required to examine adversarial manipulation, function isolation, model security, and privacy-preserving threat analysis. Overall, the proposed approach provides a conceptual foundation for developing responsive, scalable, and intelligent cybersecurity systems capable of improving threat identification and prevention in contemporary cloud computing environments.

REFERENCES

1. Al-Marri, NAAA, Ciftler, BS & Abdallah, MM 2020, ‘Federated mimic learning for privacy preserving intrusion detection’, Proceedings of 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). IEEE, pp. 1–6.

2. Almufti, Saman & Zeebaree, Subhi. (2024). Leveraging Distributed Systems for Fault-Tolerant Cloud Computing: A Review of Strategies and Frameworks. Academic Journal of Nawroz University. 13. 9-29. 10.25007/ajnu.v13n2a2012.

3. Alpernas, Kalev & Flanagan, Cormac & Fouladi, Sadjad & Ryzhyk, Leonid & Sagiv, Mooly & Schmitz, Thomas & Winstein, Keith. (2018). Secure Serverless Computing

Using Dynamic Information Flow Control. Proceedings of the ACM on Programming Languages. 2. 10.1145/3276488.

4. Andi, Hari. (2021). Analysis of Serverless Computing Techniques in Cloud Software Framework. Journal of ISMAC. 3. 221-234. 10.36548/jismac.2021.3.004.

5. Ang'udi, Janet & Awour, Stephany. (2023). Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences. 10. 155-181. 10.30574/wjaets.2023.10.2.0304.

6. Ansari, MS, Alsamhi, SH, Qiao, Y, Ye, Y & Lee, B 2020, 'Security of distributed intelligence in edge computing: Threats and countermeasures', in the cloud-to-thing continuum, Palgrave Macmillan, Cham, pp. 95–122.

7. Arulprakash&SampathKumar, K 2020, 'Improved encryption towards data security in serverless computing,' Journal of Computational and Theoretical Nanoscience, vol. 17, no. 12, pp. 5256–5260.

8. Asghar, T, Rasool, S, Iqbal, M, Qayyum, Zu, Mian, AN &Ubakanma, G 2018, 'Feasibility of serverless cloud services for disaster management information systems,' Proceedings of 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1054–1057.

9. Association, Information & Sen, Jaydip. (2015). Security and Privacy Issues in Cloud Computing. 10.4018/978-1-4666-6539-2.ch074.

10. Atifi&Bou-Harb, E2017, 'On correlating network traffic for cyber threat intelligence: A Bloom filter approach,' Proceedings of 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 384-389, IEEE, 2017.