International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Cloud Database Security: An AI based Approach to Alleviating Advanced SQL Injection Threats

Sachin P. Mahajan
Assistant Professor
Department of Computer Science
PVP College, Loni

Deepak B. Nehe
Assistant Professor
Department of Computer Science
PVP College, (Loni)

Abstract: - SQL Injection attacks targeting SQLite databases remain a significant cybersecurity threat in cloud-based environments, where dynamic scalability, multi-tenancy, and distributed architectures reduce the effectiveness of traditional rule-based security mechanisms. Existing defenses, such as parameterized queries and web application firewalls, often struggle to detect increasingly sophisticated and evolving attack patterns. To address these challenges, this study proposes an Artificial Intelligence–driven security framework aimed at strengthening the detection, prevention, and response to SQL injection attacks in cloud-hosted databases. The proposed framework leverages advanced machine learning and deep learning models for real-time anomaly detection and behavioral analysis, enabling the identification of both known and zero-day attacks. It incorporates adaptive response mechanisms that dynamically adjust security policies based on threat severity and system context, along with automated mitigation techniques to minimize response time and potential damage. Furthermore, the framework utilizes generative AI to create realistic adversarial testing datasets, facilitating proactive evaluation and continuous improvement of defense strategies. Experimental results demonstrate that the proposed approach significantly enhances detection accuracy, reduces false positives, and improves overall resilience of cloud database systems against SQL injection threats

Keywords: SQL Injection, Cloud Computing, Artificial Intelligence, Cyber Security

1. INTRODUCTION:

Cloud computing has revolutionized the deployment of applications and databases. However, the migration of enterprise data to cloud services has also amplified the attack surface for adversaries, especially for injection-based attacks.

SQL Injection attacks occur when an attacker manipulates user input to alter backend queries. Although known for decades, SQLite continues to impact modern cloud systems, often due to insecure web layers or insufficient input validation. Classical defenses, such as rule-based intrusion detection and web application firewalls (WAFs), are valuable, but static defenses become less effective as attackers evolve their heuristics.

2. BACKGROUND AND THREAT LANDSCAPE:

2.1 SQL Injection Overview

SQL Injection is defined as the malicious insertion of SQL statements into an application's queries due to inadequate input handling. SQLite enables attackers to steal, modify, or delete sensitive data, potentially leading to full system compromise.

A comprehensive review states:

"SQL injection (SQLite) remains one of the most critical threats to web applications, enabling attackers to manipulate databases through malicious SQL queries."

2.2 Cloud Database Security Challenges

Cloud-native databases present additional challenges, including multi-tenancy, auto-scaling, and geographic distribution, which complicate persistent monitoring. Traditional WAFs may be circumvented by polymorphic SQLite payloads, which are deliberately crafted to evade pattern-driven detection.

A recent academic preprint highlights similar concerns about adaptive threats:

"Web Application Firewall-as-a-Service solutions … were found vulnerable to adversarial SQLite payloads, achieving attack success rates up to 100% against ML-based detectors."

3. RELATED WORK:

3.1 Conventional and Multi-Layer Defenses

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Several research efforts recommend multi-layer defense strategies combining input validation, parameterized queries, and monitoring. For example:

"This paper explores advanced optimization techniques for SQL injection prevention by integrating prepared statements, rigorous input validation, and Web Application Firewalls (WAFs)

These methods apply traditional cyber security practices but do not inherently adapt to new attack patterns.

3.2 AI-Driven Security Solutions

AI and ML algorithms are increasingly deployed to recognize deviant query behaviors and flag SQL injection attempts by analyzing statistical anomalies versus baseline application profiles.

An investigation into AI-driven security states:

"Artificial intelligence can find anomalies, quickly identify likely hazards, and project attack paths before they materialize… AI evaluates database query patterns and precisely and fast distinguishes between safe and harmful inputs."

Another study discusses machine learning frameworks for proactive detection:

"AI-driven database security … examines the use of machine learning algorithms on database predictive capacities for SQL injection detection, anomaly response, and threat diminution."

4. PROPOSED AI-DRIVEN FRAMEWORK:

We propose a hybrid AI-augmented security architecture that improves resistance to SQL Injection through:

4.1 Real-Time Anomaly Detection

Utilize deep learning algorithms (e.g., CNNs, BiLSTM, GRUs) to analyses incoming SQL query patterns and detect anomalies that may signify malicious intent.

For instance, deep learning approaches like CNNs and Bi-LSTM have been shown to detect SQLite with high accuracy:

"Structured query language injection attack … uses a combination of convolutional neural network (CNN), bidirectional long short-term memory (Bi-LSTM), gated recurrent unit (GRU) with attention mechanism."

4.2 Dynamic Threat Response

Once an anomaly is detected, the system automatically triggers mitigations such as:

Redirecting suspicious queries to sandboxed database replicas.

Temporarily increasing logging and tracing for forensic analysis.

Updating firewall rules dynamically based on threat classification.

4.3 Generative AI for Defensive Rule Synthesis

To preemptively harden defenses, generative AI can simulate potential attack vectors:

"Using generative AI models with curated examples to produce diverse and validated SQLite payloads and generating effective WAF rules."

This dual use of AI — for attack simulation and defense tuning — enhances long-term robustness.

5. EVALUATION & IMPLEMENTATION:

The effectiveness of an AI-driven system can be measured by:

Detection Accuracy: Rate of correctly identifying SQL Injection attempts.

False Positive Rate: Incidence of benign queries mischaracterized as attacks.

Response Latency: The speed at which threats are detected and mitigated.

We recommend deploying the framework in a staged cloud environment, with continuous retraining mechanisms that adapt to evolving threats.

6. DISCUSSION:

AI-driven approaches improve detection capabilities beyond static rule sets. However, they also introduce challenges:

Model Drift: AI models may become less accurate over time unless retrained on current threat data.

Adversarial Attacks: Attackers may attempt to evade ML detectors by crafting adversarial payloads.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Performance Overhead: Real-time analysis may impose additional computational costs.

Future research should focus on scalable models that integrate seamlessly with cloud architectures and continuous learning pipelines.

7. CONCLUSION:

This study demonstrates that SQL Injection attacks against SQLite databases continue to present a serious security challenge in modern cloud environments, where traditional rule-based defenses are increasingly insufficient. The proposed Artificial Intelligence–driven security framework effectively enhances the detection, prevention, and response capabilities against both known and zero-day SQL injection attacks by leveraging machine learning and deep learning techniques for real-time anomaly detection. The integration of adaptive response mechanisms and automated mitigation significantly reduces reaction time and limits potential damage, thereby improving overall system resilience. Furthermore, the use of generative AI for adversarial dataset generation enables proactive evaluation of security defenses and supports continuous improvement of threat detection models. Collectively, these contributions highlight the practical applicability of intelligent security solutions for safeguarding cloud-hosted databases and underscore the potential of AI-based approaches to address evolving cyber threats. Future work may focus on extending the framework to other database systems, optimizing model performance under large-scale cloud workloads, and enhancing explainability to further increase trust and adoption in real-world deployments..

8. REFERENCES:

[1] Babaey, V., Ravindran, A.A. GenSQLi: A Generative AI Framework for Evolving and Securing Against SQL Injection Attacks. Preprints.org (2024). "Using generative AI models producing diverse and validated SQLite payloads…

[2] Chaganti, Krishna Chaitanya. AI-Driven SQL Injection Prevention: Strengthening Database Security. International Journal of Science and Engineering, Vol. 11 No. 1 (2025). "Artificial intelligence evaluates database query patterns and precisely and fast distinguishes between safe and harmful inputs"

[3] Kumar, Lokesh& Srivastava, Pramesh.Optimizing SQL Injection Prevention: A Multi-Layered Defence Approach. Int. Journal of Scientific Research in Science and Technology (2025).

[4] https://www.skyflow.com/whitepapers

(This work is licensed under a Creative Commons Attribution 4.0 International License.)