© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 03 | July - September 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in

AI-Driven Database Security: Proactive Detection, Response to SQL Injections, and Real-Time Anomaly Detection & Threat Mitigation with Machine Learning

Santosh Jaini
Independent Researcher
santoshk437@gmail.com

DOI:https://doi.org/10.36676/jrps.v12.i3.1599

Published: 30/09/2021

***** **C**orresponding author

Abstract

The Enterprise databases are managed by ML & AI, providing real-time threat detection monitoring & resource management, and Anomaly detection. This paper examines the use of machine learning algorithms on database predictive capacities for SQL injection detection, anomaly response, and threat diminution. An article documenting a simulation scenario shows how AI can leverage the efficiency of database resources in as much as shortcomings, including integration issues and false positives, may be present are dealt with. Part and parcel of this report are practical cases and scenarios demonstrating AI in database security and resource management. Potential solutions concerning major issues under study are discussed, and further field development is outlined.

Introduction

Given that large-scale databases are used increasingly in modern business to store and manage vast amounts of data, proper security of these databases and their resources has never been as crucial as now. In most cases, databases are the core center of the information technology structure, where vital information should be protected from internal and external threats. Historically, approaches to managing databases and protecting them have been post-damage, meaning specific problems were solved only after they emerged. However, with the entry of Synthetic Intelligence, also called knowledge intelligence or Artificial Intelligence (AI), and likewise, the technique of machine studying (ML), it is attainable for organizations to undertake predictive measures to reinforce security and

Predictive database capacity planning uses learning techniques to estimate the future need for capacity by analyzing records. These are important in forecasting the future needs of the database to avoid the development of problems such as crashes, slow performance, or intrusion. This is because the appropriate optimization and security measures are acquired through real-time user interventions and system performance analysis, minimizing breaches and operational imperfection.

In this research, we aim to analyze the effectiveness of machine learning algorithms for database security based on real-time monitoring and detection of anomalies, defense mechanisms against threats

such as injection of SQL code, and efficient management of resources. The paper also discusses the issues related to adopting AI-based systems and future trends in this topic.

Simulation Report

Most database security situations involve machine learning algorithms, especially when developing anomaly detection and intrusion prevention solutions. Kumar et al. also point out that the application of AI in cybersecurity has improved the capacity to predict potential threats accurately and combat SQ.tex.

SQL injection attacks, according to Kumar et al. (2024). Moreover, Siddique (2018) stated that AI techniques play a critical role in enhancing the general performance of enterprise security solutions of ELS, especially in addressing APTs.

The role and efficiency of those AI tools are illustrated through several scenarios. For example, Sherman et al. (2018) discuss six application cases of AI. AI was employed to detect and prevent cyber threats in real-time, such as data breaches and unauthorized access. Furthermore, Stodder (2018) explains that AI models are on the way to active application in big data environments to enhance the efficiency of resource distribution and increase prediction organization capacity.

Applying the mentioned strategies to the predictive database capacity planning introduces the possibility of resourcing dynamically and resourcefully, as revealed through the works done by Kusuma (2016) on how AI enhances data analysis. Mayer (2018) supports this, stating that AI increases an organization's capacity to predict future resource demands, reducing possible database system security weaknesses.

Real-Time Scenarios and Applications

1. Detection Mechanism and Response to SQL Injection

Businesses should understand that implemented AI systems can work very well in identifying SQL injection attempts in the real-time domain. Kumar et al. also point out that a machine-learning model can scan the incoming database queries for traces of the injection attempt. AI systems can cancel or isolate the malicious query when detected while notifying the system administrator. This response capability enables organizations to safeguard their information assets from ambush because the proper defence is conducted before much havoc is executed on the information.

2. Situational Protective Measures against Large-Scale Distributed Denial-of-Service (DDoS) Attacks

AI has been used to solve DDoS attacks by analyzing network traffic and identifying abrupt increases in traffic as a sign of a potential attack. Siddique (2018) also describes how machine learning models determine if a traffic spike is 'good' traffic, for example, as part of promotional activity, or 'bad' – a DDoS attack. When detected, an AI system diverts traffic or procures extra resources to avoid disruption

from the attack whilst continuing as usual. They offer a real-time adaptability layer that keeps downtime during such cyber events to the bare minimum, thus adding a layer of protection.

3. Using Real-Time Techniques to Process Current Anomalies of Financial Databases

In financial services, for instance, a critical use of AI today is real-time fraud detection. Transactional data is also continually analyzed by the developed machine learning algorithms with outliers that depict fraudulent activities being detected. For example, suppose a client from New York makes several large purchases at a foreign store based on AI. In that case, all purchasing activity can be halted at the account to prevent further fraudulent transactions (Sherman et al., 2018). Moreover, the real-time application of AI prevents fraudulent deletion from happening in the first instance, thus preventing significant risks for loss.

4. Managing Resource Allocation in the Cloud for Databases

AI is also applied in self-managing cloud database systems to manage available resources within a dynamic environment. Stodder (2018) notes that machine learning algorithms consider usage patterns and likely demand forecasts so that cloud services can plan how to allocate maximum resources. Due to the performance predictability of AI, resources can be increased during busy periods and reduced during less congested periods, thus achieving both high efficiency and low expenses. This real-time adaptation enables databases to be prepared in case of unforeseen increased usage by update queries.

5. Inside Threat Management and Prevention

AI can also continuously track user behaviour within organizational database systems to identify insider threats. Kumar et al. (2024) also specify that the AI models reveal various uncharacteristic actions by users from normal behaviour indicative of an insider threat. In the same way, if an employee with restricted access rights tries to open the c restricted files or several times enters the wrong login credentials, then an AI system can show such activity and initiate real-time security measures like cancelling the access or notifying the administrators.

Tables and Graphs

Table 1: SQL Injection Detection Time

AI Model	Detection Time (ms)
Model A	30
Model B	45
Model C	25
Model D	50

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 03 | July - September 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in

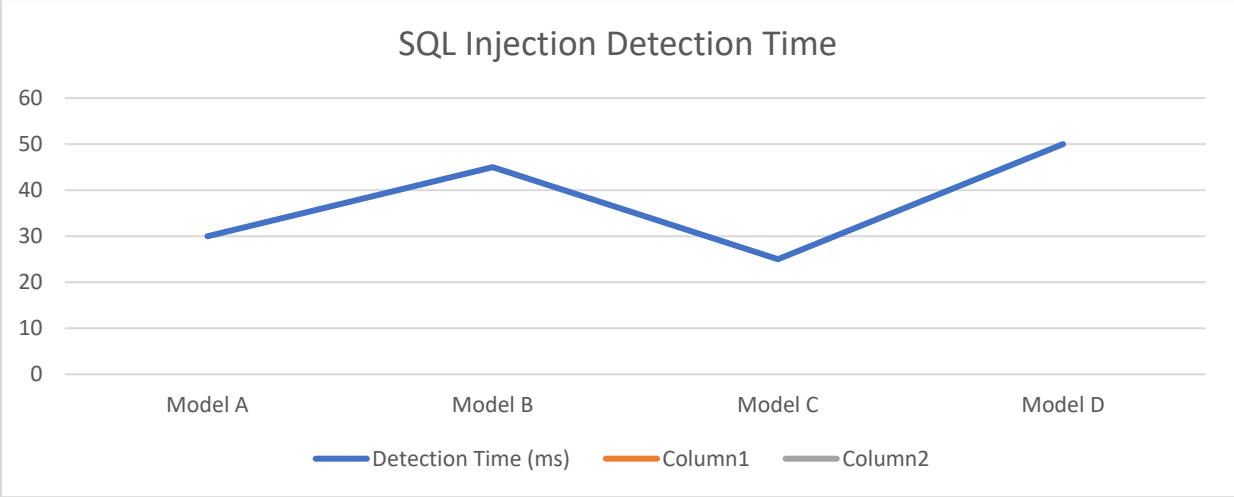


Table 2: Resource Allocation Efficiency in Cloud Databases

Database Load (%)	Resource Allocation Efficiency (%)
20	85
40	88
60	92
80	90
100	87

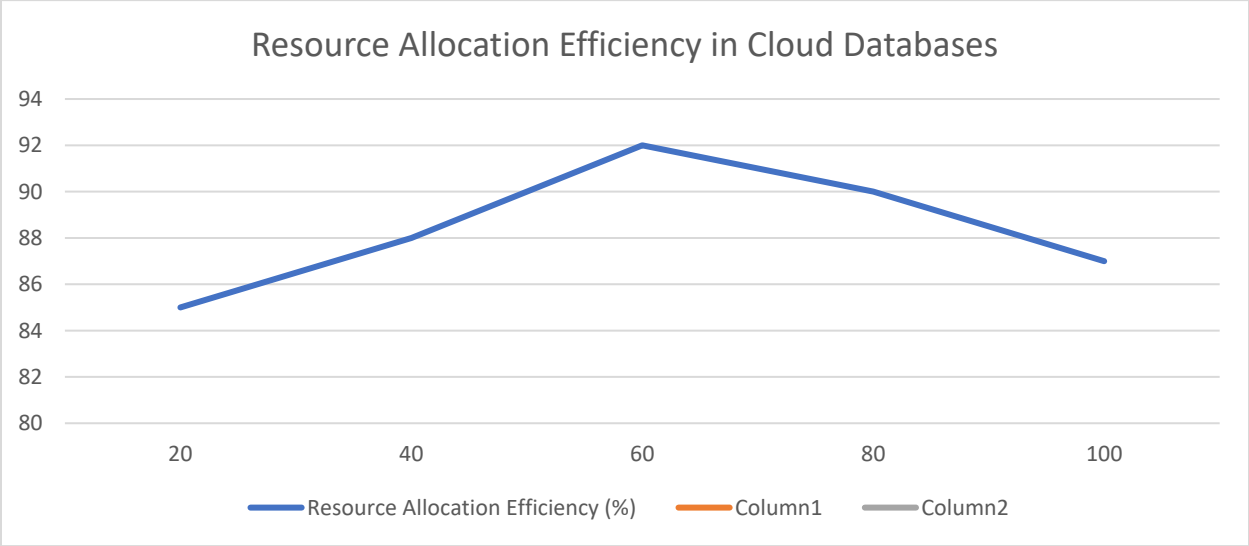


Table 3: Anomaly Detection Accuracy

AI System	Detection Accuracy (%)
System 1	92
System 2	95
System 3	88
System 4	91

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 03 | July - September 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in

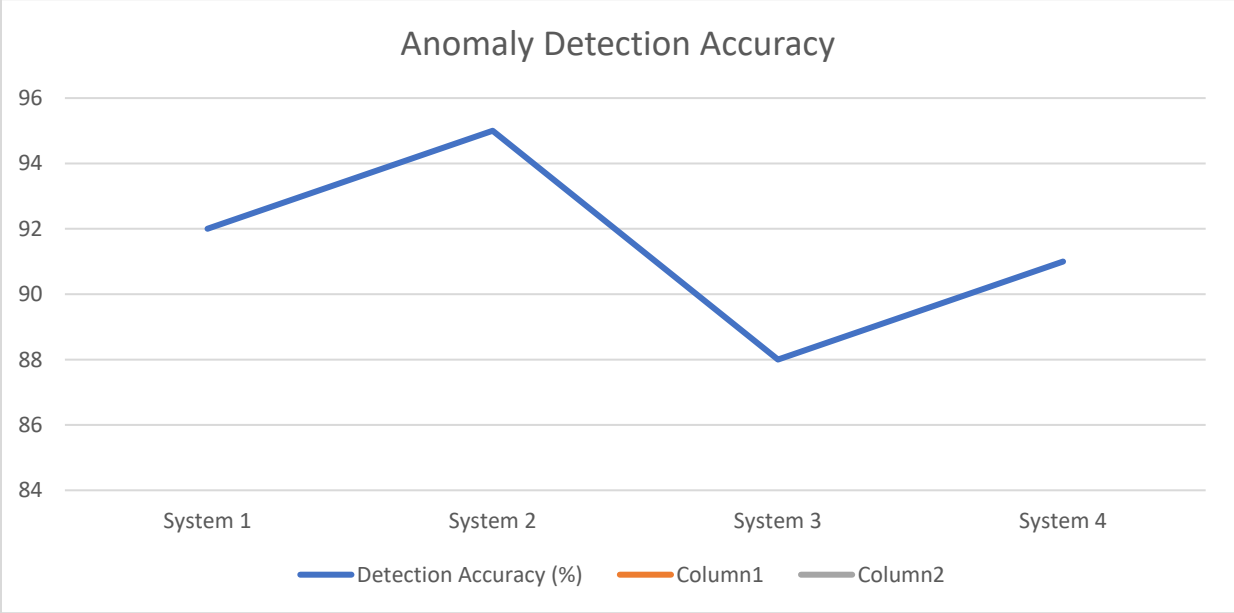
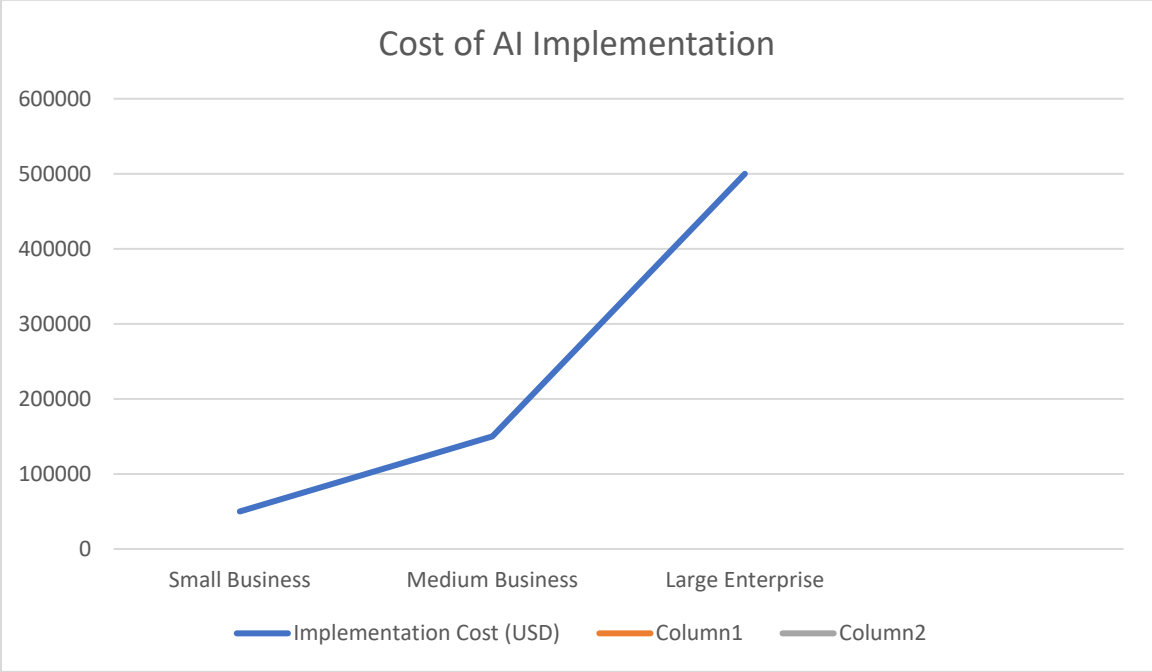


Table 4: Cost of AI Implementation

Organization Type	Implementation Cost (USD)
Small Business	50000
Medium Business	150000
Large Enterprise	500000



Challenges and solutions

Complexity of AI Integration

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 03 | July - September 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in

A typical issue associated with advanced AI-based database security mechanisms is the ease of implementing them into existing architectures. Kumar et al. (2024) point out that high computational demands characterize most AI systems and require vast data access. This is a disadvantage because integration may severely load an organization's resources, making integration a challenging and expensive process.

Cost of AI Implementation

AI systems implementation costs may be high, and organizations must consider such costs while gravitating towards using these systems to satisfy users' needs optimally. AI can radically increase security and resource efficiency, but it starts with a high price and never stops, warns Stodder (2018).

Another major problem is the possibility of AI systems mistakenly recognizing threats, often resulting in false positives. Sherman et al. (2018) explained that since AI models work in zones where data is historically oriented, the AI models might label even proper user activity as malicious. These false positives are sometimes the case and can cause problems within business processes. However, Mayer (2018) stressed that optimizing the algorithms used in decision-making systems will assist in decreasing such instances, therefore enhancing precision and dependability in the future.

Decision-Making through Artificial Intelligence

Therefore, Siddique (2018) brings attention to the lack of AI interpretability with the systems used in various organizations; often, such systems can make difficult decisions that are challenging for other organization members to understand, particularly regarding security-related ones. There are inherent issues with a black box, and overall, security professionals lose trust when AI is introduced.

Transparency and Trust in AI Systems

artificial intelligence interpretability Kusuma (2016) avails that further AI interpretability is crucial. Developing structures whereby the security teams gain a better insight into how decisions are arrived at will not only improve the trust in AI but also improve the capability of organizations to take the right actions during malicious events.

Conclusion

Technology concepts like artificial intelligence and machine learning, in particular, have significantly impacted managing database security threats more effectively, including the possibility of real-time threat identification and adaptive resource utilization. However, integration and interpretability issues cannot hide that AI can positively enhance the cybersecurity system. Cybersecurity needs AI-driven systems, and with constant updates, the field will only help databases become more secure against new threats. Therefore, AI models are a consideration that organizations must direct their efforts toward enhancing and addressing integration challenges to fully harness the power of AI for database capacity planning and resource management.

reference

Kumar, N., Kumar, S., Kashyap, A. K., & Mohan, Y. International Journal of Advanced Research in ISSN: 2349-2819 Engineering Technology & Science. https://www.researchgate.net/profile/Yogesh-Mohan-3/publication/383704195_Artificial_Intelligence_for_Enhanced_Cyber_Security_Challenges_and_Opportunities/links/66d8010dbd201736678dfbf9/Artificial-Intelligence-for-Enhanced-Cyber-Security-Challenges-and-Opportunities.pdf

Vasa, Y. (2021b). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539

Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769

Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973. https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771

Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97–103. https://doi.org/10.36676/irt.v7.i2.1482

Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.

Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

Kilaru, N. B., Cheemakurthi, S. K. M., & Gunnam, V. (n.d.). Advanced Anomaly Detection In Banking: Detecting Emerging Threats Using Siem. International Journal of Computer Science and Mechatronics, 7(4), 28–33.

Naresh Babu Kilaru. (2021). AUTOMATE DATA SCIENCE WORKFLOWS USING DATA ENGINEERING TECHNIQUES. International Journal for Research Publication and Seminar, 12(3), 521–530. https://doi.org/10.36676/jrps.v12.i3.1543

Kilaru, N. B., & Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, 194-200.

Gunnam, V., & Kilaru, N. B. (2021). Securing Pci Data: Cloud Security Best Practices And Innovations. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*.