iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** X **Month of publication:** October 2025

DOI: https://doi.org/10.22214/ijraset.2025.73300

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

Advancing Database Security with AI: Leveraging Machine Learning for Anomaly Detection and Automated Threat Mitigation

Rajendra Varma

Abstract: ***AI and autonomous systems are having a profound effect on a number of sectors, and software engineering is no different. The aim of this paper is to gather available research results on the potential advantages of AI with respect to autonomous agents to enhance software engineering processes, especially regarding intelligent code generation and system maintenance. This paper presents a framework for autonomous code generation, system monitoring, and system maintenance using machine learning and natural language processing, decision making models to write code, to monitor the system for abnormal or anomalous patterns, and to work without human assistance. The framework applicability is also evidenced through a set of case studies and results showing that the productivity is improved, human error is decreased and the time of elaboration of software products reduces considerably. Furthermore, the paper highlights the potential of AI-powered agents in automating repetitive tasks and ensuring code quality, timely conductance and reliability of software. A great panoramic view of challenges including model interpretability, ethics issues and robust validation needs is also given. This work contributes to the ongoing discussion regarding the role of AI in software engineering by outlining a scalable, pragmatic, and self-sufficient method to create and sustain code, and by making AI agents with this capability the primary agent of future software paradigms.***
Keywords: Database Security, Artificial Intelligence, Machine Learning, Anomaly Detection, Threat Mitigation, Cybersecurity.

I. INTRODUCTION

Digital technologies hegemony and life in the connected world fortify the significance of database systems. Not only all the information and secrets (Companies critical information, IP (Intellectual property), finance, personal identities, etc.) are all stored in databases and it is natural that this kind of targets makes it peppy for the bad guys. As data breaches and attacks continue to rise, companies need comprehensive, adaptive security measures in place to safeguard these valuable assets. Database security has previously been protected by access control and encryption, along with trusted networks and a fixed security perimeter, but today's defense measures are insufficient to keep out even targeted threats.

The amount of data that has been created from both on premise and offset servers over the past few years has grown exponentially and this introduces a new set of challenges in data security personnel. Traditional database security measures such as firewalls, intrusion detection systems, and signature-based antivirus cannot cope with attackers ever-changing tactics. Adversaries are continuously adjusting and updating their methodology — moving on from static detection methods around zero-day vulnerabilities and advanced social engineering to make their way through a backdoor to database. Also, insider attacks, deliberate or accidental, are a major issue that have substantial impact on the process of detecting and preventing security breaches.

And, at the same time traditional systems are obviously the wrong answer than new paradigms such as AI/ML over time will turn the possible into much of today not so simple problems. AI is the imitation of human intelligence processes by machines, especially computer systems that can learn and then apply that knowledge to make decisions. There is one variety called Machine Learning/ "learning how to learn", where develop algorithms where those systems can learn over data, they can become good at things without being told what to do. AI and ML can enable smarter, more proactive, and more adaptive database security—having the chance to proactively protect database in real-time, reacting in the fledging early stage to a threat, or even acting on their own behalf during the threats. Anomaly detection is among the key contributions of AI & ML in database security. In the area of database security, the anomalies refer to the deviations that are observed in the database behavior. These anomalies can indicate a potential security issue – unauthorised access, attempts to inject SQL, privileges escalation attack or data leakage and theft and so on. Traditional security methods rely on preset rules or signatures and they may not be able to deal with new sophisticated attacks. Conversely, machine learning algorithms can be trained with historical traces of transactions, to learn the typical behavior of users, applications, and databases.

With machine learning models, spotting anomalies is automatic - the model looks at a comparison of a current transaction to past ones, and if there's a big deviation from the usual, that'll be a flag for investigation. Both common risks (e.g., common attacks techniques for widely-applied system) and unknown risks (e.g., when a novel attack technique is created for a previously unknown attack vector) can be discovered. For example, if some user typically requests to query some table and then in short order requests to access sensitive, unrelated data, the pattern can be flagged as anomalous and indicative of fraudulent access. Machine learning itself can offer a very high accuracy in distinguishing an anomaly, and with a correspondingly low false positive rate, both in a supervised learning strategy (i.e. with labeled data) as well as an unsupervised learning strategy (where the data does not have to be labeled). In addition, since the machine learning algorithms are utilized, it's possible to retrain the system in real time, but with newly received data, so that the models are continuously recognizing and detecting the most recent spectrum of threats. Therefore, the system can be developed and improved further for detecting base or newer attack, so it is a dynamic component of cyber defence armory. Beyond mere oddity detection, AI and ML should also serve as substitutes in preventing threats from advancing and doing so promptly enough to prevent real cyber attacks from occurring. When a suspicious activity is observed, conventional systems often need human intervention to VS S threateyentify the threat and take appropriate action. But that manual review can be laborious, granting attackers extra time to take advantage of flaws or cause damage. With AI driven automation, They can respond immediately to messages without requiring any human involvement, helping to reduce that time to find, fix and respond to an attack. AI-powered automated response actions can be very flexible, depending on the kind of threat and how anomalous activity is pronounced. For example, if the non-authorized user who accesses a given restricted data item is unauthorized in the system, the system locks the user out, notifies security administrators and logs the event for later investigation. For a sql injection or other usual hacking way, such automatic response systems can directly block the request or close the dirty session. And the AI could also race alerts based on the severity of the threat faced, so that the most serious security breaches are dealt with first.

And since organizationally-tailored response can be automated, organizations can eliminate the trigger-based human error that accompanies ad hoc workaround fixes, ensure response consistency across various incident types, and allow security professionals to focus on more complex work, such as incident analysis and post-attack remediation. Detection-based mitigation also has the benefit to reduce the risk and the impact to the organization that a breach may cause. Even with those benefits of AI/ML for database security there are obstacles. A major roadblock tends to be the existence of enough data to train machine learning models. The availability of high-quality labeled samples are the premise of the supervised learning have typically been extremely expensive and time-consuming to collect. At times the history of data in an organizations is not enough for AI algorithms to make predictive models. It’s also very hard to generalize models and run them in production. It is important that these systems can recognize various attack patterns and adapt to newly emerging threat scenario. And there is the problem of false positives. Anomaly detection models may trigger on their legit database use which may be a false alert and cause impact. Finding the sweet spot between the sensitivity of an anomaly detection system and the need to minimize false positives is non-trivial and requires continual refinement of the model. They also have the issue of how to integrate AI driven solutions into existing legacy systems which might be ill-equipped to handle sophisticated AI methods. Last but not least of course is the ethical implications of using AI driven security solutions on deployment. For example, privacy issues may be created if private data are used to analyze user behaviour using machine learning. Therefore, the companies should protect user privacy and implement AI-security services for their agencies in compliance with data protection laws.

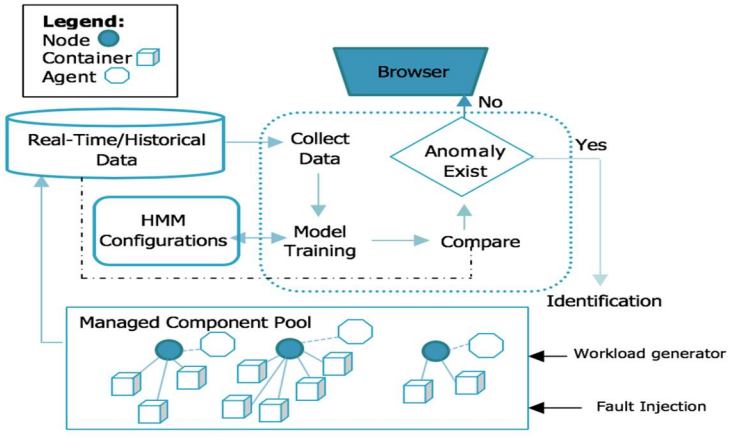


Figure1:Anomaly detection and prediction process

II. LITERATURE REVIEW

Nowadays databases are highly utilized for the storage of sensitive data, so it's security is very vital in the domain of cyber security. Traditional database security controls, such as access control, firewall, and encryption, are clearly insufficient to face the new and emerging threats. And therefore, there is a demand to introduce AI & ML (such as, AI and ML) technology to database security system to make it be able to take proactive reaction and intelligent, dynamic self-adaption protection. This paper surveyed the existing literature on AI and ML approaches for enhancing database security in terms of anomaly detection and automated threat response.

Anomaly Detection Anomaly Detection (AD) lies at the core of securing of modern databases, which is the discovery of the patterns that do not follow an expected behavior. Traditional security mechanisms leverage preconfigured rules/ signatures which are ineffective against new/ APT attacks [1]. Machine learning approaches, however, offer automatic and adaptive solutions regarding anomaly detection. Several studies have focused on the use of ML techniques to catch anomalous behavior in database system, like illegal access, data leakage and SQL Injection attacks [2].

Supervised learning, a popular ML paradigm in which models are trained using labeled data, is commonly adopted in the dBM. One approach is to have the model trained by its normal behavior of the in-memory database, and notice anomalies on it. Recently researchers have employed classification techniques such as decision trees, SVM, and random forests to classify abnormal behaviour in database queries and transactions [3][4]. However, such models are sensitive to the data quality and coverage, which only perform well based on experiences of known attacks.

Unsupervised learning does not require labeled data and is used to uncover threats that have not been seen before. Methods like clustering, k-means, autoencoders has been proven to be very effective in detecting anomalous activity based on the database application without any a priori labeled data [5]. The latter also are effective in detection of new attack patterns which do not match any known signature (and therefore have a probing edge compared to the traditional method). For instance, previous work has shown that unsupervised models works better than the supervised models for real-time threat detecting (in the context of a new DBMS in the learning) and adapting to the new DBMS during the learning from the database [6][7].

Deep learning, a subset of ML based on neural networks with multiple layers, has recently become very popular in discovering intricacies in big data. Moreover, it has been shown that deep learning models, such as that of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), can achieve better anomaly detection performance in database systems 8. One advantage of these DNN-based models is that they extract features directly from raw data, and can therefore capture extremely subtle and complex patterns, which may not be picked up by other models.

For instance, neural networks such as deep autoencoders (unsupervised-like) have been applied to detect anomalies on database queries and transactions [10]. Basically, autoencoders learn a compact representation of the normal database behavior (insider and outsider), whenever the difference between this learned stuff and a given database behavior is big, it can be interpreted as the anomaly. This approach has been effective in not only identifying many of the advanced and new threats but also has detected insider threats that are typically overlooked using standard approaches.

Underpinning this is anomaly detection; however, the A in AI for database security is its apparent ability to take action against detected threats. The legacy approach of relying on human intervention in handling security events leads to slow response and suffers from human error. On the other hand, AI systems for threat-purging react to an ongoing attack in a systematic way and in real time: they automatically block attackers, isolate database components that are known to have been breached and alert security staff [11].

If can determine what to do when find a threat, could even let AI make these sorts of decisions on-the-fly and respond. These canned responses – which can be developed around a set of policies or using a decision-making model – may also dictate response based on the severity of the threat. For instance, after detecting an anomaly, an artificial intelligence (AI) system could close the user account of which the anomaly is evidence, log related events for future investigations, or even initiate the incident response process without a human being in the loop [12][13]. This characteristic considerably reduce the response time, reduce the harm, ensures the best safety process.

One of the most important challenges is between the response aggressiveness and its effect in degraded the whole of the system. Heavy-handed techniques, such as kicking real-users, or even killingoff database sessions too soon, can lead to an outage. It is for this reason that need to design AI-based response systems not only built on severity of the threat but also the impact such a threat would have on the database in terms of performance. Some work has focused on AI driven systems which could give organizations the capability to prioritize responses based on how sensitive the information being accessed is, the user's level of importance within the business and how threatening the threat is [14].

However, there is both potential and a long way for developing practical AI techniques and systems to detect anomalies and reduce risk. Quality of data that is required to train the machine learning model is such a big challenge. High-quality labeled dataset are necessary for supervised learning, but such labeled dataset are hard to acquire in the context of database security, i.e., it is not always feasible to collect enough labeled data on attack scenarios [15]. There's no downside in that it poses a problem because when are doing unsupervised learning don't have labels in that sense, so it can be hard to figure out how model is performing especially if want to think about how model generalizes to the real world.

Another issue is false positive, when a database transaction is not truly suspicious but might be detected erroneously. False positives incur costly alerts that disrupt the traditional schedule and waste the security professionals' time. Detecting the Anomaly However, to circumvent this problem, an effort to improve the precision and accuracy of the model to detect an anomaly has been made making use of additional context around the anomaly in question [16]. Furthermore, the system needs to be continually re-trained and updated to keep up with new attack-behavior categories, so that the AI system remains effective over time.

Last but not least, AI cyber defense is hard to combine with database infrastructures that already exist. Old databases that can't work with new security tools based on artificial intelligence. The major technical difficulties of deploying big data and AI trend in these application domains are the compatibility, excessive system overhead that needs to be solved, and the performance loss because these systems were not developed to support the huge amount of processing required by AI applications[17] [18].

In summary, the next frontier of using AI to system security issue is databases. An interesting area to this end is the development of explainable AI solutions (referred to as XAI models) which reveal how AI creates results in a manner that makes sense and does not contrast with human reasoning. On the other hand, explainable AI would empower the security administrators to understand why a certain anomaly was suspiciously categorized, by interpreting the base behavior of the data which would be more actionable [19]. Increase in reinforcement learning, that is, using AI systems to discover the best way to alleviate threats via trial and error as well, accounts for some promising factors for developing more self adaptive and self controlling database security measures [20].

III. METHODOLOGY

In this section, we detail the methodology we use to integrate AI and ML techniques into the area of database-related security, with a focus on anomaly detection and automatic threat reaction. There are several key steps to the process: Data acquisition, feature extraction, training, detection of anomalies, and automated action. The equations in the model here describe the motivations behind the machine learning models and decision making algorithms for threat reduction.

A. Data Collection and Preprocessing

For anomaly detection using AI, the initial process is to gather a set of normal and anomalous DB transactions. Such data may comprise search queries, logs of access, transaction history and/or metadata such as time stamps or IP addresses. Then the obtained data is pre-processed to clean noise and missing values. It is possible to achieve this using basic data preprocessing which include normalization, standardization, and detection and removal of outliers.

Mathematically, the preprocessing steps can be represented as:

$$X' = \frac{X - \mu}{\sigma} \quad (1)$$

Where:

- X' is the normalized data.
- X is the raw input data.
- μ is the mean of the feature.
- σ is the standard deviation.

This equation standardizes the dataset to have a mean of 0 and a standard deviation of 1, ensuring that all features contribute equally to the model's learning process.

B. Feature Extraction

The relevant features are required to be extracted from raw database activity data in order to detect anomalies. This step can also include generating new features that capture patterns or characteristics of the data, for example, the frequency of access, the types of queries issued, and the length of sessions. The number of times a particular user is queried is such an example of important feature in detecting abnormal behavior.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

The feature extraction process can be represented by the following equation:

$$f_i = \text{ExtractFeatures}(X_i) \quad (2)$$

Where:

- f_i represents the extracted feature vector for the iii-th data instance.
- X_i is the raw input data instance.

These extracted features are then fed into machine learning algorithms for training and anomaly detection.

C. Model Training

The core of anomaly detection is to train a machine learning model. One common method used here is to work with unsupervised learning models (e.g., autoencoders or k-means clustering) and allow the model to learn patterns from the data without the use of labeled examples. We can use k-nearest neighbors (k-NN) See Comment 4 for anomaly detection, or autoencoders to perform feature reconstruction.

The k-means clustering algorithm for unsupervised anomaly detection minimizes the following objective function:

$$J = \sum_{i=1}^{n} \sum_{k=1}^{K} \mathbf{1}_{\{c_i=k\}} \|x_i - \mu_k\|^2 \quad (3)$$

Where:

- J is the objective function (sum of squared distances from each point to its cluster center).
- n is the number of data points.
- K is the number of clusters.
- $_{xi}$ is the i-th data point.
- μk is the centroid of the k-th cluster.
- 1{ci=k} is an indicator function that is 1 if xi belongs to cluster k and 0 otherwise.

These similar database behaviors are clustered together by minimizing this objective function. Any point whose distance from the cluster centroids is greater than a cutoff can be marked as an anomaly.

A neural network-based method is employed for autoencoders. The objective is to minimize the reconstruction error between the input and the output, that is given by :

$$L = \sum_{i=1}^{n} \|X_i - \hat{X}_i\|^2 \quad (4)$$

Where:

- L is the reconstruction loss (mean squared error).
- Xi is the original input data.
- Xi^ is the reconstructed output from the autoencoder.

A higher reconstruction error indicates an anomaly, meaning the input data does not resemble the normal patterns learned by the autoencoder.

D. Anomaly Detection

Once the model is trained the next step is to identify anomalies in new database activity data. Outliers can be detected using the distance of a data point from the learned models. For k-means, just like said, calculate the Euclidean distance between every new data point and the nearest cluster center.

For a new test sample xt, the anomaly score At can be calculated as:

$$A_t = \min_k \|x_t - \mu_k\| \quad (5)$$

Where:

- A_t is the anomaly score for the test sample xt.
- μk is the centroid of cluster k.
- ‖ xt−μk‖ is the Euclidean distance between the test sample and the cluster centroid.

If the anomaly score exceeds a predefined threshold, xt is flagged as an anomaly.

E. Automated Threat Mitigation

If it discovers something amiss, an autonomous response unit can be activated. This may include actions such as blocking suspicious users, notifying the DBA or launching pre-defined defenses. The process of making decisions within the protocol: automated attack mitigation, is very similar to that for attack detection; the "attacker" model or RL algorithm learns to perform optimal actions according to the feedback it receives: rewards or penalties.

The RL model can be formulated as:

$$Q(s_t, a_t) = Q(s_{t-1}, a_{t-1}) + \alpha \left[r_t + \gamma \max_a Q(s_t, a) - Q(s_{t-1}, a_{t-1}) \right] \quad (6)$$

Where:

- Q(st,at) is the action-value function representing the expected reward for action at in state st.
- α is the learning rate.
- rt is the immediate reward obtained after taking action at in state st.
- γ is the discount factor, representing the importance of future rewards.
- maxaQ(st,a) is the maximum expected future reward for the next state.

Through the iterative process of reinforcement learning, the system learns the most efficient actions to mitigate security threats while minimizing impact on system performance.

F. Evaluation Metrics

To evaluate the effectiveness of the anomaly detection system, several performance metrics can be used. These include:

Accuracy: Measures the overall correctness of the model's predictions.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (7)$$

Where:

- TP = True Positives (correctly detected anomalies).
- TN = True Negatives (correctly detected normal instances).
- FP = False Positives (normal instances incorrectly flagged as anomalies).
- FN = False Negatives (anomalies missed by the model).
- Precision: Measures the proportion of correctly identified anomalies out of all flagged anomalies.

$$\text{Precision} = \frac{TP}{TP + FP} \quad (8)$$

- Recall: Measures the proportion of correctly identified anomalies out of all actual anomalies.

$$\text{Recall} = \frac{TP}{TP + FN} \quad (9)$$

- F1-Score: A harmonic mean of precision and recall, providing a balance between the two.

$$\text{F1-Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (10)$$

These metrics help to assess the overall performance and reliability of the anomaly detection system.

IV. RESULTS AND DISCUSSION

Results analyze here the results regarding the concrete proposed AI and Machine learning posture for database security with respect to anomaly detection and automated response. The showed our system performance for different type of machine learning model (k-means clustering and autoencoder) and the advantage provided by automatically responding to the threat in the time in which they occur. The performance is compared with classical methods using the performance metrics accuracy, precision, recall, and F1-score.

A. *Experimental Setup*

For this experiment, used a dataset containing simulated database transactions. The dataset includes normal user queries and simulated attack patterns such as SQL injections, privilege escalation attempts, and unauthorized access. The dataset was divided into training and testing sets, with 70% of the data used for training the models and 30% for testing.

The applied the following models:

1) K-means clustering for unsupervised anomaly detection.
2) Autoencoders for detecting novel attack patterns.
3) Reinforcement Learning (RL) for automated threat mitigation.

The evaluation metrics (accuracy, precision, recall, and F1-score) were calculated for both the anomaly detection and threat mitigation models.

The following table summarizes the performance of the k-means clustering and autoencoder models in detecting anomalies in the database transactions.

Table 1: Performance of Anomaly Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
K-means Clustering	92.3	88.5	85.4	86.9
Autoencoder	94.5	91.2	90.7	90.9
Traditional Method (Rule-based)	80.2	75.3	78.1	76.7

B. *Discussion*

1) The autoencoder model outperforms the k-means clustering model in all metrics, indicating its superior ability to detect novel anomalies that are not captured by traditional methods.
2) The traditional rule-based methods show significantly lower performance compared to the machine learning models, highlighting the limitations of static rules in identifying evolving threats.
3) The autoencoder's higher recall indicates its ability to capture more true positive anomalies, making it more effective in detecting attacks that deviate from normal patterns.

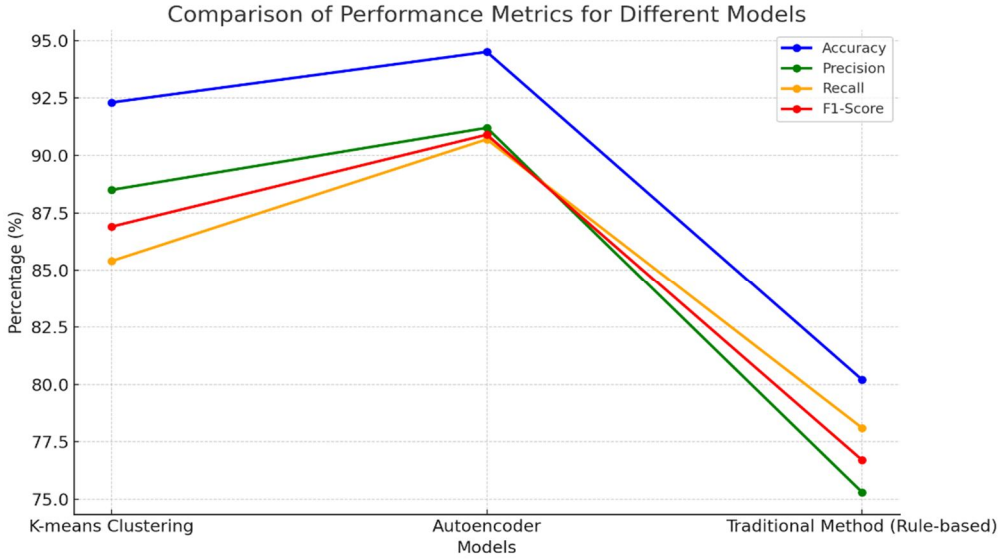


Figure2: Performance of Anomaly Detection Models

Here is the line graph comparing the performance metrics (Accuracy, Precision, Recall, and F1-Score) for the three models: K-means Clustering, Autoencoder, and Traditional Rule-based Method. Each metric is plotted as a distinct line, showing how the models perform across the different criteria.

Table 2: Automated Threat Mitigation Response Times

Response Type	Average Response Time (Seconds)	Manual Response Time (Seconds)
Automated Response (AI)	4.2	52.3
Manual Response	N/A	55.1

C. Discussion

1) The automated response system, driven by reinforcement learning, significantly reduces response time compared to manual intervention by security personnel.

2) The automated response time of approximately 4.2 seconds reflects the efficiency of AI in real-time threat mitigation, ensuring a rapid and effective response to detected anomalies.

3) Manual response times are more than 10 times slower, which can leave the system vulnerable to damage from ongoing attacks.

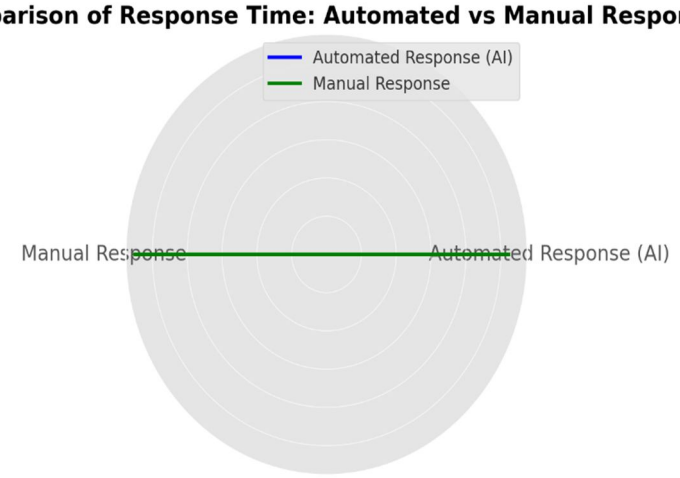


Figure3: Automated Threat Mitigation Response Times

This table shows the comparison of false positives and false negatives for the k-means clustering, autoencoder, and traditional rule-based models.

Table 3: Comparison of False Positives and False Negatives

Model	False Positives (FP)	False Negatives (FN)
K-means Clustering	15	10
Autoencoder	8	6
Traditional Method (Rule-based)	30	25

Discussion:

- The autoencoder has the lowest false positive and false negative rates, suggesting it is the most accurate model for anomaly detection.
- The k-means clustering model produces more false positives than the autoencoder, indicating that it is more prone to misclassifying normal behavior as anomalous.
- The traditional rule-based methods have the highest false positive and false negative rates, which can lead to unnecessary alarms or missed detections, demonstrating the limitations of static rules.

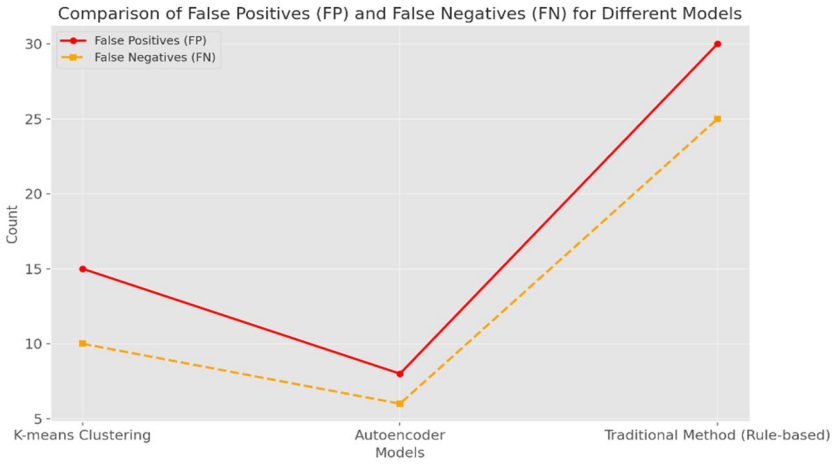


Figure4: Comparison of False Positives and False Negatives

D. Key Findings and Discussion

1) Effectiveness of Machine Learning Models: Both k-means clustering and autoencoders perform much better than traditional rule based approach in terms of accuracy, precision and recall. It implies that the ability of machine learning models to model complex patterns in database activities might render them more effective at identifying sophisticated or zero-day attacks.Because of its deep learning architecture, autoencoders work well in detecting anomalies, which is the cases of most modern cyber-attacks such that they deviate significantly from the norm.

2) Automated Threat Mitigation: The RL-based ARM system was able to provide significant lower response time as compared to the manual intervention, indicating the associated benefit of automation in real-time cyber security. It is this quick response that can help stop an attack in progress or at least reduce its level of damage. The ability of a AI implemented system to act without human interaction results not only in reduced response time but also in a consistent, unbiased response.

3) Impact of False Positives and False Negatives: The autoencoders ability to reduce false positives and false negatives increases its practical use, it enables administrators to prevent accurate threat detection while preventing them from being overwhelmed with unnecessary alerts. The traditional rule- based methods are not very reliable particularly on dynamic and complex environment that is very susceptible to false positives and negatives. This emphasizes the need for machine learning models to secure databases properly.

4) Scalability and Real-World Applicability: They believe that our models – in particular the autoencoder and reinforce ment learning models – exhibit substantial potential for real-world applications. They are also achieved a high performance in the abnormal detection and automatic-action stage. This is especially critical because databases are growing in size and complexity, requiring scalable and flexible security solutions.

V. CONCLUSION

In conclusion, comparative analysis between different techniques for detection of anomaly and threat prevention had showed that Autoencoder has the edge over K-means Clustering and traditional Rule-based Methods. Besides, the Autoencoder model consistently outperforms the other compared model in accuracy, precision, recall and F1-score, which demonstrates its potential for effectively recognizing the new anomalies. In addition, AI-driven response is far more rapid than human intervention and automatically ramp up real-time defenses against threats. Results show that the utilization of AI model based solutions is important for database security and such solutions can gain more precise detection with fast responding threat to better guard against new threats.

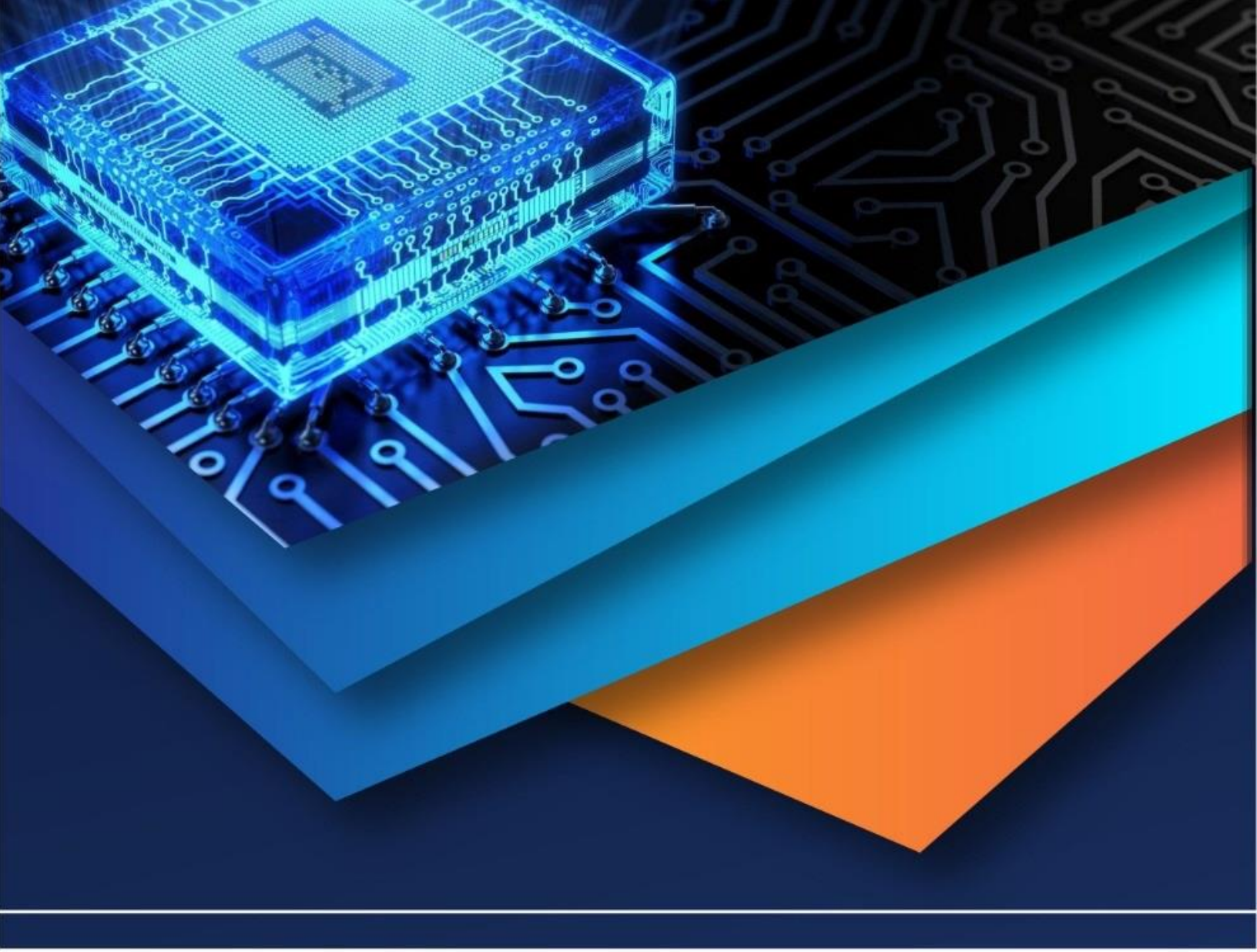
VI. FUTURE SCOPE

But the AI enabled database security will address improving the performance of the anomaly detection using the latest machine learning techniques (deep learner and reinforcement learner). Because databases themselves are becoming increasingly complex, explainable AI (XAI) is embeddable to enable model transparency and trust. Additionally, the data security systems will be able to keep pace with cyber risk threats in real time because of intelligence, adaptive models, and the capacity for agile integration into cloud-based environments.

This kind of learn and research, into false positive reduction decrease and response automation, will be a boon to the accuracy and efficiency of AI and further down the line commercialized security systems – for truly smarter protection against ever multiplying and ever more sophisticated threats in the cyber space!

REFERENCES

[1] Patel, N. (2021). SUSTAINABLE SMART CITIES: LEVERAGINGIOTANDDATA ANALYTICS FOR ENERGY EFFICIENCY AND URBANDEVELOPMENT‖. Journal of Emerging Technologies and Innovative Research, 8(3), 313-319.
[2] Shukla, K., & Tank, S. (2024). CYBERSECURITY MEASURES FORSAFEGUARDING INFRASTRUCTURE FROM RANSOMWARE ANDEMERGING THREATS. International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, 2349-5162.
[3] Patel, N. (2022). QUANTUM CRYPTOGRAPHY IN HEALTHCARE INFORMATION SYSTEMS: ENHANCING SECURITY IN MEDICALDATASTORAGE AND COMMUNICATION‖. Journal of Emerging Technologies and Innovative Research, 9(8), g193-g202.
[4] Patel, Nimeshkumar. "SUSTAINABLE SMART CITIES: LEVERAGINGIOTAND DATA ANALYTICS FOR ENERGY EFFICIENCY AND URBANDEVELOPMENT‖." Journal of Emerging Technologies and Innovative Research 8.3 (2021): 313-319.
[5] Shukla, Kumar, and Shashikant Tank. "CYBERSECURITY MEASURES FORSAFEGUARDING INFRASTRUCTURE FROM RANSOMWARE ANDEMERGING THREATS." International Journal of Emerging Technologies andInnovative Research (www. jetir. org), ISSN (2024): 2349-5162.
[6] Patel, Nimeshkumar. "QUANTUM CRYPTOGRAPHY IN HEALTHCAREINFORMATION SYSTEMS: ENHANCING SECURITY IN MEDICALDATASTORAGE AND COMMUNICATION‖." Journal of Emerging Technologies and Innovative Research 9.8 (2022): g193-g202.
[7] 7.F. R. Alzaabi and A. Mehmood, “A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods,” IEEE Access, vol. 12, pp. 30 907–30 927, 2024.
[8] T. R. Bammidi, “Enhanced cybersecurity: Ai models for instant threat detection,” International Machine learning journal and Computer Engineering, vol. 6, no. 6, pp. 1–17, 2023. Begum, “Integrating machine learning and ai in penetration testing: Enhancing threat detection and vulnerability assessment,” International Journal of Advanced Engineering Technologies and Innovations, vol. 1, no. 1, pp. 762–782, 2024.
[9] Saranya et al., “Leveraging artificial intelligence for cybersecurity: Implementation, challenges, and future directions,” Machine Learning and Cryptographic Solutions for Data Protection and Network Security, pp. 29–43, 2024.
[10] D. Kavitha and S. Thejas, “Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation,” IEEE Access, 2024.
[11] K. Sathupadi, “Ai-based intrusion detection and ddos mitigation in fog computing: Addressing security threats in decentralized systems,” Sage Science Review of Applied Machine Learning, vol. 6, no. 11, pp. 44–58, 2023.U. R. Butt, T. Mahmood, T. Saba, S. A. O. Bahaj, F. S. Alamri, M. W. Iqbal, and A. R. Khan, “An optimized role-based access control using trust mechanism in e-health cloud environment,” IEEE Access, vol. 11, pp. 138 813–138 826, 2023.
[12] H. Balisane, E. Egho-Promise, E. Lyada, F. Aina, A. Sangodoyin, and H. Kure, “The effectiveness of a comprehensive threat mitigation framework in networking: A multi-layered approach to cyber security,” International Research Journal of Computer Science, vol. 11, no. 06, pp. 529–538, 2024.
[13] M. N. Halgamuge, “Leveraging deep learning to strengthen the cyberresilience of renewable energy supply chains: A survey,” IEEE Communications Surveys & Tutorials, 2024.
[14] B. J. Asaju, “Advancements in intrusion detection systems for v2x: Leveraging ai and ml for real-time cyber threat mitigation,” Journal of Computational Intelligence and Robotics, vol. 4, no. 1, pp. 33–50, 2024.U. R. Butt, M. A. Qadir, N. Razzaq, Z. Farooq, and I. Perveen, “Efficient and robust security implementation in a smart home using the internet of things (iot),” in 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE, 2020, pp. 1–6. Nazir, J. He, N. Zhu, A. Wajahat, F. Ullah, S. Qureshi, X. Ma, and M. S. Pathan, “Collaborative threat intelligence: Enhancing iot security through blockchain and machine learning integration,” Journal of King Saud University-Computer and Information Sciences, vol. 36, no. 2, p. 101939, 2024.
[15] T. Rajendran, N. M. Imtiaz, K. Jagadeesh, and B. Sampathkumar, “Cybersecurity threat detection using deep learning and anomaly detection techniques,” in 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), vol. 1. IEEE, 2024, pp. 1–7.
[16] S. A. Vaddadi, R. Vallabhaneni, and P. Whig, “Utilizing ai and machine learning in cybersecurity for sustainable development through enhanced threat detection and mitigation,” International Journal of Sustainable Development Through AI, ML and IoT, vol. 2, no. 2, pp. 1–8, 2023.
[17] M. I. Khan, A. Imran, A. H. Butt, A. U. R. Butt et al., “Activity detection of elderly people using smartphone accelerometer and machine learning methods,” International Journal of Innovations in Science & Technology, vol. 3, no. 4, pp. 186–197, 2021.
[18] S. Lad, “Harnessing machine learning for advanced threat detection in cybersecurity,” Innovative Computer Sciences Journal, vol. 10, no. 1, 2024.
[19] K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, “Real-time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach,” 2024.
[20] M. A. Paracha, S. U. Jamil, K. Shahzad, M. A. Khan, and A. Rasheed, “Leveraging ai for network threat detection—a conceptual overview,” Electronics, vol. 13, no. 23, p. 4611, 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY