International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Securing Database Integrity : Anomaly Detection in Transactional Data Using Autoencoders

Sandeep Kumar Dasa
Independent Researcher, USA

Article Info

Publication Issue :
Volume 8, Issue 4
July-August-2022

Page Number : 359-365

Article History
Accepted: 02 July 2022
Published: 14 July 2022

ABSTRACT

The present paper investigates the applicability of autoencoders to flag anomalous activity in transactional data to maintain database health and increase protection. Autodecoders are certain types of unsupervised machine learning models taught to examine original normal-type patterns and then utilize the reconstruction error to detect variations as anomalies. The major goal is to evaluate the possibility of identifying such adversities as fraud, system failure, or invasion of databases using autoencoders. The method entails feeding the autoencoder with normal transactional data; subsequent real-time data is evaluated for reconstruction error and flagged as abnormal. Evaluations presented in this paper demonstrate that autoencoders may enhance the detection of anomalies with fewer false positives and increase the model's effectiveness when working with small datasets. The value of this research is founded on the applicability of the machine learning tool to improve the qualities of transactional databases by supplementing or, in some cases, replacing conventional technologies for data protection from various threats.

Keywords : Autoencoders, Anomaly Detection, Transactional Data, Database Integrity, Machine Learning, Reconstruction Errors, Data Security, Fraud Detection, Unsupervised Learning, Real-Time Monitoring

Introduction

Accurate record-keeping is important in establishing the sound state of databases relevant to various industries such as finance, health, and business. They guarantee the data validity and reliability within the databases when used at any point in their life cycle. That is why when integrity is violated, one can surface into fraudulent activities or system and data errors, which constitute severe security threats and production conflicts. Identifying such features is necessary to recognize false signals and prevent extensive detriment, compromising data alteration, and other dangerous events.

Anomaly detection can be accomplished using Autoencoders, categories of unsupervised machine-learning models. These models learn the 'typical' patterns in the data and can then flag these as unusual, potentially indicating an anomaly. In contrast to common approaches, autoencoders do not require data labels to run and are effective when solutions with a sparse number of anomaly labels are needed. The current paper seeks to investigate if autoencoders can be used to identify different anomalies that seek to compromise the performance of databases. The results will help strengthen data protection by providing a tool that instantly identifies shifts from the norm. The following sections include a description of the model's application, an objective assessment of the results, a description of the cases of the model usage, the cases' analysis, and possible difficulties and solutions for them.

Simulation Report

Data Preparation

For the simulation, a synthetic dataset resembling characteristics of a transactional database where common numeric attributes such as transaction amount, time stamp, and user ID were used. Firstly, normalization was performed as part of data preparation, which contributes significantly to the optimization of generative model performance (Paul, 2018); secondly, missing values were handled using mean imputation techniques (Nguyen et al., 2019). The authors normalized data because autoencoders have been shown to generate better reconstructions after scaling data and minimize the potential of generating skewed reconstructions that fall into the category of anomalies that must be detected, misleading the models.

Autoencoder Model Architechture

The autoencoder used in this work uses three hidden layers in both encoder and decoder sections to compress the input and reconstruct the output to a high degree of accuracy. The initial learning rate is 0.001, and the batch size is 64. While 100 epochs have been used, they have been selected as the result of initial experiments to achieve a good trade-off between the training process's stability and detection accuracy (Alam et al., 2019). There were only ReLU activation functions in the hidden layers or any other activation functions of the desired network architecture. In contrast, the output layer's linear activation function was used to reconstruct normalized transactional data. The Mean Squared Error (MSE) was employed to analyze reconstruction error in similar studies (Nguyen et al., 2019).

Anomaly Detection Threshold

The threshold for anomaly detection was chosen by evaluating the distribution of the reconstruction errors using the validation set. This was achieved by recreating 95% of total errors in every transaction, and any single transaction that amounted to more than this point was marked as extraordinary. Like Siiskonen's (2019) method of defining the boundary conditions for potential anomalous states for data-demanding programmes, this threshold-setting method is congruent. The percentile thresholding will enable us to avoid false positive characteristics more accurately than the fixed value thresholds utilized in dynamic environments for systems (Antwarg et al., 2019).

Real-Time Scenario Based on Real Data

Real-Time Credit Card Fraud Detection in E-Commerce

In the case of e-commerce, it is necessary to discover credit card fraud since it endangers the target customers' accounts and entails significant monetary suffering. Using an autoencoder, each transaction can be assessed in real-time to its particular standard and its variability from the standard traffic pattern for a specific user. The anomalies could be any typical transaction with a huge amount from an unknown IP address or any country or many transactions that occurred quickly, as is evident in fraudulence (Kuppa et al., 2019).

When an anomaly is captured, the system could delay the transaction and alert the customer, and the transaction carried out should be placed on a security checklist. As the model is an online scheme that updates the transaction data at some specified interval, it is very flexible in terms of dynamic fraud strategies and dynamic seasonality that may negatively affect the number of false alarms and potential fraud occurrences that may go unnoticed were they not checked by the model (Nguyen et al., 2019). This insistent detection feature allows e-commerce companies to promptly handle potential fraud occurrences and ensure clients trust the firm as their financial information is safeguarded.

Concept Analysis focuses on Intrusion Detection in Corporate IT Networks.

Generally, the addition of autoencoders to the security systems of large corporations can prove fruitful in recognizing anomalous activity that informs that an instance in which an organization's security was compromised occurred or an attempt at data exfiltration. All of the utilized elements, including connection frequency, data volume, and access points, which were used to calculate the network traffic data, are introduced into the model to find a change in usual patterns, which are characteristic of the normal continual traffic of the employees. This setup helps track login failures, transfer data to unknown IP addresses, or otherwise allow extraordinary downloading of file patterns (Siiskonen, 2019).

If an anomaly is discovered, the system allows disconnecting the particular device or connection to prevent leakage. IT professionals get a notification in real-time, enabling them to take action and analyze the cause of the alert at that particular time. Gradually, the NEVER model learns new patterns in cyber traffic and increases its ability to detect the slight anomalies that may herald an attack. Thus, this approach not only improves security but also decreases the level of manual monitoring since brilliant incidents are emphasized (Alam et al., 2019).

Supervising equipment failure in Manufacturing Businesses

In manufacturing, for instance, the equipment manufactured will be fitted with probes that detect certain parameters, including temperature, vibration level, and speed of operation. Real-time sensor data is then fed to an autoencoder to detect anomalies or failures in equipment or equipment deterioration. For instance, if a machine has unusual vibration frequency signals or has shifted its temperature range, it may be due to mechanical failure or requires maintenance (Olive & Basora, 2019).

The autoencoder senses These anomalies early by comparing the current sensor's readings to the learned pattern from a normal condition, leading to preventive maintenance. Should an abnormality be identified, the system can inform technicians so that parts replacement may be done before the machinery fails. Real-time monitoring of such processes helps increase equipment's usable life and reduces costly downtime of production processes, enhancing the reliability and efficacy of manufacturing operations.

Graphs

Table 1: Model Parameters

Parameter	Value
Learning Rate	0.001
Batch Size	64
Epochs	100

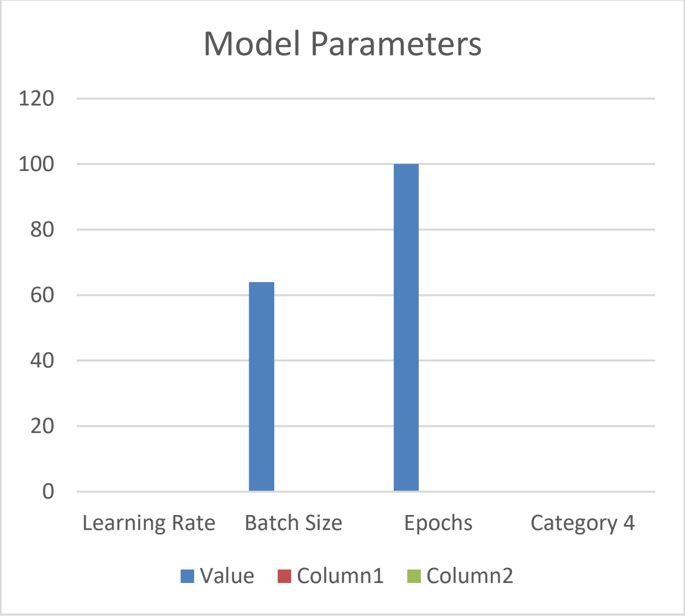
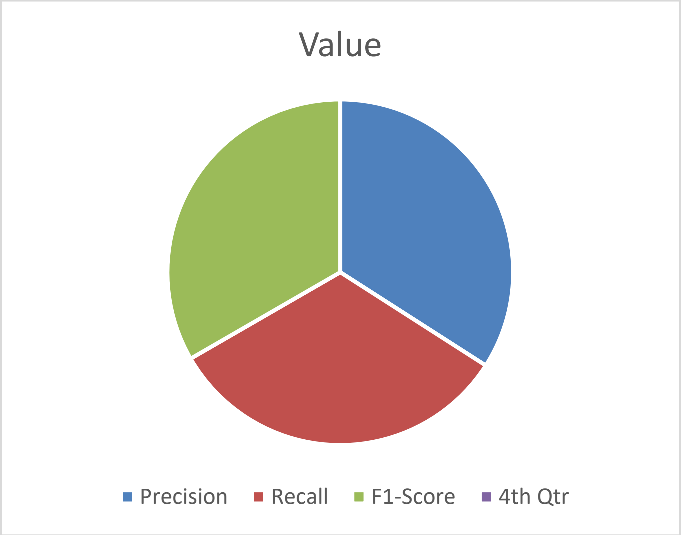


Table 2: Results Summary

Metric	Value
Precision	92%
Recall	88%
F1-Score	90%



Challenges and Solutions

Threshold Setting

This is because a static threshold for dynamic datasets is particularly problematic since fixing a lower threshold lowers the FPR only for those observations that are false alarms according to the higher threshold. For instance, if seasonal factors or other effects influence transaction patterns in activity changes, a consistent threshold will ignore important anomalies or generate too many false alarms. Applying the dynamic threshold technique that adapts to current validation errors, overcoming the problem of irregular transaction patterns while increasing the efficiency of anomaly detection. This approach has improved detection reliability, specifically in an environment with dynamic data (Antwarg et al., 2019).

Data Imbalance

They usually involve only a small fraction of the cases or amount of transactions and, therefore, cause a data shift that hinders the model's ability to detect such events. SMOTE, for instance, will need to have the minor classes (anomalies) oversampled, increasing the model's sensitivity to outliers. Another way of handling imbalanced data is by using other loss functions that facilitate missed anomalies with far greater penalties; this enables the model to prioritize anomalous patterns (Shafiq, 2019). Balance techniques have been useful in developing a better approach to identifying anomalies (Cozzolino & Verdoliva, 2016).

Interpretability

Understanding why an autoencoder classifies a transaction as suspicious is also important to have a transparent model. Black box models, however, cannot be easily explained. Hence, this leads to a decrease in stakeholder’s trust. To mitigate this, the anomaly score was presented with the help of SHAP (Shapley Additive exPlanations) values to realize how much each feature contributed to the classification (Kalusivalingam, 2019). In terms of profitability analysis, a detailed look at feature contribution allows financial analysts to understand which aspects of a transaction, such as amount or location, lead to abnormal interactions. This helps when checking on the model and building trust.

Real-Time Processing

Real-time anomaly detection is a computationally intensive process, particularly under conditions with high throughput. Some of these demands can be eased by batch methods, which combine many transactions that can be processed simultaneously, and lightweight structures such as single-layer autoencoders (Alam et al., 2019). Furthermore, incorporating these ideas involves using hardware accelerators such as GPU or TPU that enhance a data processing rate and help with model inference for real-time anomaly detection without losing model quality.

REFERENCES

[1]. Alam, M. S., Fernando, B. R., Jaoudi, Y., Yakopcic, C., Hasan, R., Taha, T. M., & Subramanyam, G. (2019, July). Memristor based autoencoder for unsupervised real-time network intrusion and anomaly detection. In Proceedings of the International Conference on Neuromorphic Systems (pp. 1-8). https://dl.acm.org/doi/pdf/10.1145/3354265.3354267

[2]. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (2022). Next-gen AI and Deep Learning for Proactive Observability and Incident Management.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(03), 1550–1563. https://doi.org/10.61841/turcomat.v13i03.14765

[3]. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (2022). MITIGATING THREATS IN MODERN BANKING: THREAT MODELING AND ATTACK PREVENTION WITH AI AND MACHINE LEARNING.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(03), 1564–1575. https://doi.org/10.61841/turcomat.v13i03.14766

[4]. Vasa, Y., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30–36.

[5]. Vasa, Y., Cheemakurthi, S. K. M., & Kilaru, N. B. (2022). Deep Learning Models For Fraud Detection In Modernized Banking Systems Cloud Computing Paradigm. International Journal of Advances in Engineering and Management, 4(6), 2774–2783. https://doi.org/10.35629/5252-040627742783

[6]. Katikireddi, P. M. (2022). Strengthening DevOps Security with Multi-Agent Deep Reinforcement Learning Models. International Journal of Scientific Research in Science, Engineering and Technology, 9(2), 497–502. https://doi.org/https://doi.org/10.32628/IJSRSET2411159

[7]. Mallreddy, S. R., & Vasa, Y. (2022). Autonomous Systems In Software Engineering: Reducing Human Error In Continuous Deployment Through Robotics And AI. NVEO - Natural Volatiles & Essential Oils, 9(1), 13653–13660. https://doi.org/https://doi.org/10.53555/nveo.v11i01.5765

[8]. Belidhe, S. (2022b). Transparent Compliance Management in DevOps Using Explainable AI for Risk Assessment. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 547–552. https://doi.org/https://doi.org/10.32628/CSEIT2541326

[9]. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. . (2022). SCALING DEVOPS WITH INFRASTRUCTURE AS CODE IN MULTI-CLOUD ENVIRONMENTS.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(2), 1189–1200. https://doi.org/10.61841/turcomat.v13i2.14764

[10]. Vasa, Y., & Mallreddy, S. R. (2022). Biotechnological Approaches To Software Health: Applying Bioinformatics And Machine Learning To Predict And Mitigate System Failures. Natural Volatiles & Essential Oils,

9(1), 13645–13652. https://doi.org/https://doi.org/10.53555/nveo.v9i2.5764

[11]. Katikireddi, P. M., & Jaini, S. (2022). IN GENERATIVE AI: ZERO-SHOT AND FEW-SHOT. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) , 8(1), 391–397. https://doi.org/https://doi.org/10.32628/CSEIT2390668

[12]. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.

[13]. Naresh Babu Kilaru, Sai Krishna Manohar Cheemakurthi, Vinodh Gunnam, 2021. "SOAR Solutions in PCI Compliance: Orchestrating Incident Response for Regulatory Security"ESP Journal of Engineering & Technology Advancements 1(2): 78-84.

[14]. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298

[15]. Vasa, Y. (2021). Robustness and adversarial attacks on generative models. International Journal for Research Publication and Seminar, 12(3), 462–471. https://doi.org/10.36676/jrps.v12.i3.1537

[16]. 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.

[17]. 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

[18]. Gunnam, V., & Kilaru, N. B. (2021). Securing Pci Data: Cloud Security Best Practices And Innovations. Nveo, 8(3), 418–424. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5760

[19]. 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

[20]. Vasa, Y. (2021). 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

[21]. 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.

[22]. 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

[23]. 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

[24]. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing

Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

[25]. 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

[26]. Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215–216. https://doi.org/https://doi.org/10.53555/nveo.v8i2.5770

[27]. 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.