Chakradhar Bandla[1]

Harnessing Generative AI for Anomaly Detection in Distributed Cloud Databases

Journal of Electrical Systems

Abstract:
Due to the integral complex structures and distributed architecture of cloud databases, such databases are now easily prone to numerous forms of anomalies that make operational continuity and data integrity difficult. These challenges are aggravated by the environment that the cloud databases are placed in: dynamic and growing large-scale; this makes the simple anomaly detection not effective for real-time systems. The purpose of this research is to propose a new model for anomaly identification inside the generative AI class. The model would learn the subtle changes in data patterns and system behavior by utilizing the characteristics of VAEs. This way, the approach presents a proactive and efficient mechanism of anomaly since it involves the modeling of normal operation and identifying a variation. The effectiveness of the proposed model is very high; hence it can be easily implemented for real-time monitoring and mitigation for cloud services. The analysis of the obtained results points out that this solution not only improves the scalability and fault tolerance of the distributed cloud databases, but also increases the security characteristics of the databases while focusing on the important problem of the intelligent and self-tuning anomaly detection in the modern cloud systems.

Keywords: Generative AI, Anomaly Detection, Distributed Cloud, Databases

1. INTRODUCTION

Distributed cloud databases have revolutionized modern data management systems, making them more scalable, flexible, and accessible in a variety of settings. However, anomalies, which can disrupt operations and undermine data integrity, become more vulnerable as the complexity of these systems increases. The dependability and safety of cloud-based systems are greatly compromised by anomalies in distributed databases, which include abrupt changes in data patterns or unexpected actions taken by the system [1]. A crucial need exists for intelligent and adaptable solutions since traditional anomaly detection approaches often fail to keep up with the high-volume data environments that are intrinsic to distributed systems, which are dynamic and unpredictable.

A potentially useful tool for dealing with these issues is generative AI, and more specifically Variational Autoencoders (VAEs). A strong framework for real-time detection of small anomalies can be provided by VAEs, which are able to learn and model complex, high-dimensional data distributions. Generative models are able to detect and address anomalies before they become major problems because, unlike traditional methods, they can capture complex data interdependencies [2].

The Rise of AI in Anomaly Detection

Statista predicts that by 2030, the artificial intelligence (AI) market would have grown from its 2023 valuation of 241.8 billion USD to about 740 billion USD. The development of AI and ML has completely altered the landscape of conventional anomaly detection techniques. Artificial intelligence (AI) powered systems are great at sorting through massive datasets, finding complicated patterns and outliers with astounding precision, in contrast to laborious and frequently impractical human analysis. Artificial intelligence's revolutionary effects allow companies and enterprises to make better decisions based on data-driven insights, which improves the efficiency of anomaly detection operations and expands its applicability across many areas [3].

[1] Information Technology
University of the Cumberlands
chakradhar.b907@gmail.com

Importance in various industries

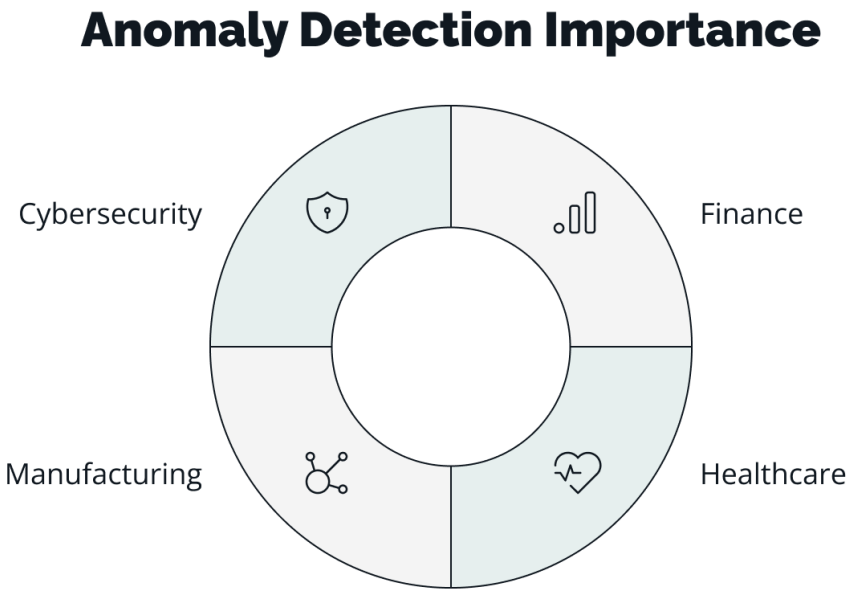

Fig 1: Importance of Anomaly Detection

Figure 1 shows the widespread use of anomaly detection across many industries, attesting to its critical importance and adaptability:

Finance

To prevent monetary losses and guarantee compliance with regulations, AD (anomaly detection) systems are used in the financial sector to spot suspicious trading patterns and fraudulent transactions [4].

Healthcare

Using AD approaches, healthcare organizations can improve patient care and operational efficiency by identifying atypical patient records. These records could signal potential health issues or data entry errors.

Manufacturing

Predicting and preventing possible problems in manufacturing equipment with real-time anomaly monitoring can save expenses and downtime.

Cybersecurity

Security breaches, susceptible data protection, and system integrity maintenance all depend on AD's ability to detect odd network activity.

Challenges and considerations

Anomaly detection with AI can have certain drawbacks, though. Data quality, data dynamics, finding the sweet spot between sensitivity and specificity, and making sense of the results are all major challenges. In addition, ongoing R&D is required to enhance the accuracy and relevance of AD systems due to the fast-paced growth of data and patterns [5].

Developed with distributed cloud databases in mind, this article introduces a new approach for anomaly detection that uses generative artificial intelligence. A scalable and efficient method for preserving operational integrity is offered by the suggested technique, which makes use of VAEs to examine data and system behavior. Aligning

with the changing demands of modern data-driven environments, our research enhances the robustness and security of cloud computing systems by overcoming the limits of classic anomaly detection techniques [6].

Where to use AI Anomaly Detection in 2024

Cybersecurity

Artificial intelligence anomaly detection is a strong defense against new cybersecurity threats. Artificial intelligence systems are able to spot unusual or subtle indicators of intrusion because they constantly monitor network traffic and user actions. This skill is absolutely necessary for:

- Intruder detection in computer networks
- safeguarding sensitive information

Fraud detection

Artificial intelligence anomaly detection is very useful in the financial industry, especially for detecting and avoiding fraudulent activity [7]. By 2027, the financial sector is expected to have spent 97 billion USD on artificial intelligence. Artificial intelligence systems can identify suspicious activity by studying user behavior and transaction patterns, which allows them to:

- Finding instances of fraudulent transactions
- Reducing potential dangers and monetary setbacks

Healthcare

Artificial intelligence anomaly detection revolutionizes healthcare by keeping an eye on patient data for indications of illness or anomalies. With this preventative method of illness identification, we are able to:

- Keeping an eye on patient records for the first indicators of illness
- Identifying unusual health problems in their infancy

Industrial systems

To keep operations running smoothly and safely in the industrial sector, AI-driven anomaly detection is essential by:

- Making accurate predictions about when machinery will break down
- Maximizing productivity

Predictive maintenance

Predictive maintenance enables, in a manner closely connected to its uses in industrial systems, to:

Optimal asset use and life extension

- Decrease maintenance expenses
- Predict maintenance needs

2. LITERATURE REVIEW

The rapidly developing field of cybersecurity has piqued the interest of researchers in artificial intelligence and related fields. Cyberattack detection, reaction, protection, and recovery have been the subject of numerous studies in an effort to address these challenges [8]. The convergence of artificial intelligence and cybersecurity has been the subject of several recent assessments. By keeping an eye on a variety of cyber threats and quickly evaluating millions of events, AI can provide analytics and insight to protect against cyberattacks that are always changing. This allows for the proactive avoidance of problems. Whether it's to automate security tasks or supplement human security teams, AI is finding more and more uses in cybersecurity.

Nevertheless, as far as we are aware, no exhaustive study has been published that delves into the most recent findings in order to elucidate the cybersecurity tasks that AI techniques address and the specifics of their implementation. In the future, researchers and industry professionals may benefit from this comprehensive overview of AI use cases in cybersecurity, which is why this systematic review set out to provide just that. Adapting and applying AI for cybersecurity also comes with research difficulties, which we covered in detail.

2.1. Cybersecurity

The term "cybersecurity" describes the methods and tools used to protect computer networks and the data stored on them against dangers including hacking, data loss, and illegal access.

Cyber risks are always changing, and the situation is already complicated due to the quick rate of technical progress and innovation. In light of this new threat, cybersecurity solutions powered by artificial intelligence have surfaced to assist teams in reducing vulnerabilities and enhancing protections [10]. To evaluate the research on AI for cybersecurity, a uniform taxonomy is required due to the heterogeneity of AI and cybersecurity. Researchers and practitioners alike will benefit from this taxonomy since it will facilitate consensus on which technological procedures and services could be enhanced using AI to bolster cybersecurity. The goal here was to learn about the different types of solutions needed to avoid, detect, react to, and survive attacks using a famous cybersecurity architecture developed by NIST [11]. Any company can improve its network security by following the guidelines laid out by the National Institute of Standards and Technology's (NIST) cybersecurity framework. Functions, classifications, subclassifications, and illuminating references make up the four main components of the structure. The AI use cases that were discovered were categorized using the first two levels of the NIST framework. On these tiers, you'll find five different cybersecurity functions and twenty-three different solution types. The functions cover the whole cybersecurity lifecycle. In order to find examples of how AI could improve cybersecurity, you can start by looking at the solution categories provided for each function. Utilizing these two levels allows for a more transparent and intuitive organization of the current literature on AI for cybersecurity into the most relevant solution categories. By outlining appropriate AI-based use cases for each level, the proposed taxonomy adds a third, compatible level to the cybersecurity framework.

2.2. Artificial intelligence

An artificial intelligence system can be defined in several ways depending on (a) its application area and (b) its lifecycle phases, which include research, design, development, deployment, and use. A popular, albeit simplified, definition of AI is used in this study because of its emphasis on AI applications for cybersecurity: In order to accomplish predetermined objectives, "systems that display intelligent behavior by analyzing their environment and with some degree of autonomy take actions" [12]. In a practical sense, artificial intelligence encompasses a wide range of technology and applications. Situations in the environment can be described as desirable or undesirable, and actions can be assigned to sequences, according to AI use cases in cybersecurity.

This SLR makes use of the artificial intelligence taxonomy that was put forth by [13], which specifies the core and transversal subdomains and domains of AI. The most important parts of AI research—reasoning, planning, learning, communications, and perception—were considered to be of utility.

While optimization and searching are aspects of planning, reasoning primarily focuses on knowledge representation and other reasoning approaches. A subfield of machine learning, perception focuses on processing sounds and computer vision, communication on understanding natural language, and learning overall [14]. Among the many branches of AI that make up this field are: topics covered include natural language processing, image analysis, object identification, case-based reasoning, planning graphs, deep learning, sentiment analysis, artificial neural networks, text mining, and sensor networks. There is a large body of literature discussing AI from several perspectives, including technical, operational, practical, and philosophical ones; the subject spans numerous academic disciplines. This study primarily focuses on the techniques and AI applications mentioned above, as well as their possible effects in cybersecurity situations. The use of artificial intelligence (AI) solutions to issues in the cybersecurity area, including identification, protection, detection, reaction, and recovery, are among the topics covered.

2.3 Automated threat hunting

Automated threat hunting involves proactively searching an organization's networks, endpoints, and datasets for suspicious, harmful, or otherwise unsafe activity. It uses newly acquired threat intelligence on previously collected data to anticipate and classify potential dangers. An emerging field of application, threat hunting is playing a crucial role in early detection. Existing approaches depend on anomaly-based threat detection, even though open-source cyber threat intelligence (OSCTI) offers a treasure trove of external threat information [15].

2.4 Data leakage prevention

Identifying and preventing data breaches, exfiltration, or unauthorized data destruction is the focus of data leakage prevention. Automated data sensitivity detection, monitoring data movement and user activity, and advanced persistent threat (APT) identification are all ways in which data can be kept safe from leaking thanks to AI approaches [16].
Data leakage prevention can be effectively achieved by keeping tabs on authorized individuals and their sensitive information usage habits. In order to detect any abnormal behavior, such as an increase in activities or unexpected conduct, researchers are presently employing AI algorithms to track user activity and compare data from various sources. In order to find out how to prevent data breaches, researchers are utilizing the CERT insider threat test dataset. This dataset contains things like daily activity summaries, email contents, the email network, and representations of user behavior throughout time. Nevertheless, Al-shehari and Alsowail [18] developed a model that can only be used to detect instances of data leakage at the critical time leading up to an employee's departure from a company.

After an incident has occurred, forensic analysis can be used to piece together when and how the attack happened, how big the breach was, where it originated, and what measures were taken to stop it from happening again. In addition to gathering evidence to support a prosecution, this investigation helps put the pieces of the puzzle together that the attacker left behind. The incident response team can benefit from AI in several ways, including intelligent attribution, forensic timeline anomaly identification, evidence correlation across devices, and an optimization framework for forensic investigation decision-making [19].

In order to determine the source of security incidents, intelligent attribution seeks to establish relationships between different entities and events. Utilizing contextual based learning allows for the recording of the present state and the provision of attribution hints.

It is possible to have a better understanding of what happened before, during, and after a cyber incident by consulting a forensic chronology. If a security incident is recorded in the forensic timeline, it is necessary to identify an anomaly. To find out what's typical in log files, you can use a deep autoencoder to generate a baseline model. Then, using the built baseline as a basis, you can set an anomalous threshold for the reconstructed data [20].

3. METHODOLOGY

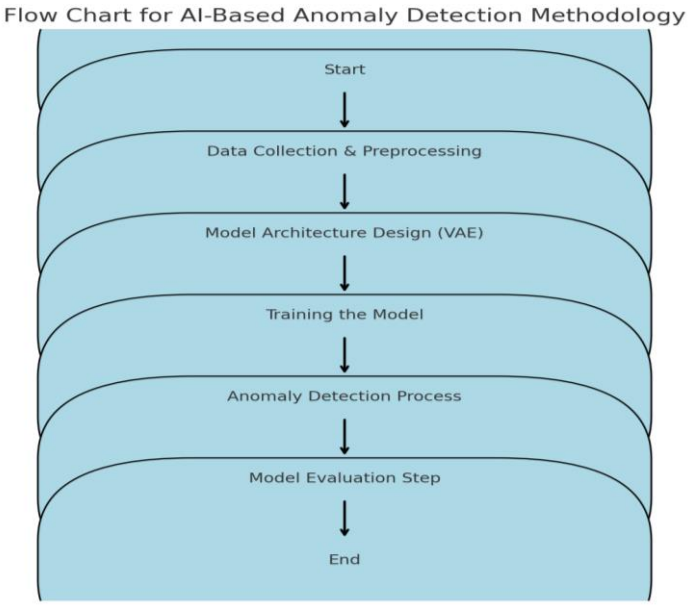

Fig 2: Flow chart of AI Anomaly detection process.

The flow chart of the Anomaly detection of AI using Anomaly detection chart is illustrated in the figure below as the flow chart of figure 2. This research puts into practice a real-time Generative AI-based Variational Autoencoder (VAE) model for distributed cloud database anomalies. The methodology comprises the following steps:

3.1 Data Collection and Preprocessing:

The data was collected from distributed cloud databases maintaining system logs, traffic generated through the network, and transactions for an airy understanding of system's behavior. First a dataset pre-processing was done to clean the data to prevent a scenario during model training where a program complains of missing values in attributes, noisy data among others that affects the entire training process. This was important in making the data more suitable for further analysis and for performing anomaly detection.

3.2 Model Architecture:

- **Variational Autoencoder (VAE)**: Designed a VAE with:
  - An encoder to map input data into a latent space representation.
  - A decoder to reconstruct the original data from the latent space.
- The reconstruction error between input and output is used as an anomaly score.
- Tuned hyperparameters (e.g., number of layers, latent space dimensions, and activation functions) for optimal performance.

3.3 Training:

Normal operating data was used to train the Variational Autoencoder (VAE) to learn the normal distribution of healthy systems. An adaptive learning rate was used during training to make it easier to converge and minimize the probability of fitting in the model to the training data set. It made the model easy to generalize, and when an anomaly was present, it easily pointed out small variations from the expected values.

3.4 Anomaly Detection:

The developed Variational Autoencoder model was used for the selected computations to be performed in real-time monitoring mode to supervise the functioning of the systems. This was done by means of variance which an adaptive threshold over the reconstruction error to detect deviations from normality. This was further enhanced by the integration of the model with cloud databases for getting the automation of the flagging and logging of the anomalous events to provide a real-time anomaly detection system.

3.5 Evaluation:

During model evaluation, all the modern metrics were included for the purpose of assessing the anomalies detection, including Precision, Recall, F-measure, and ROC-AUC analysis. Furthermore, the proposed solution was compared with conventional anomaly detection techniques, including k-means clustering and isolation forest, to confirm the increased efficiency, accuracy, and adaptability of the method for detecting various patterns of deviations in distributed cloud databases.

4. RESULTS AN DDISCUSSION

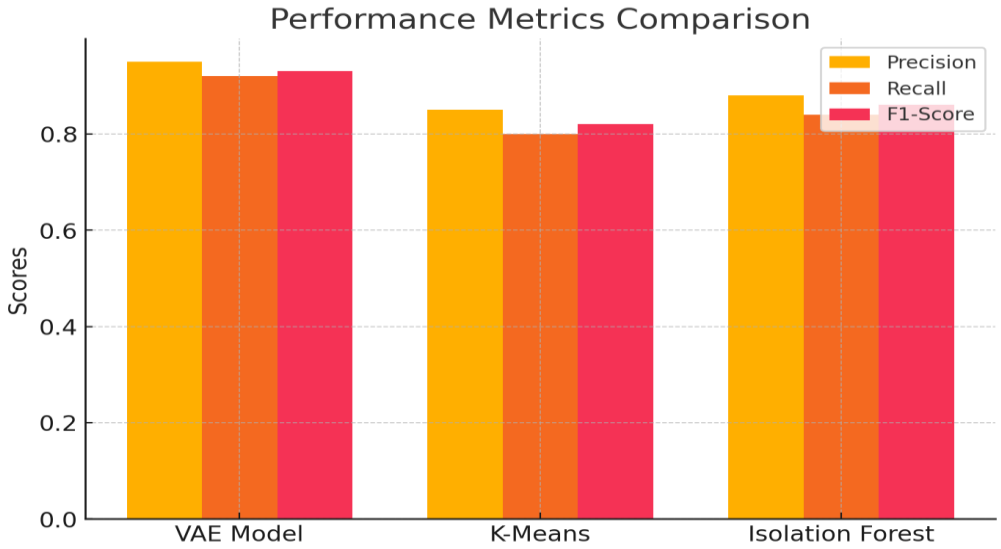

Fig 3: Performance Metrics Comparison

The VAE-based model outperforms traditional methods like k-means and isolation forest in terms of precision, recall, and F1-score is shown in figure 3.

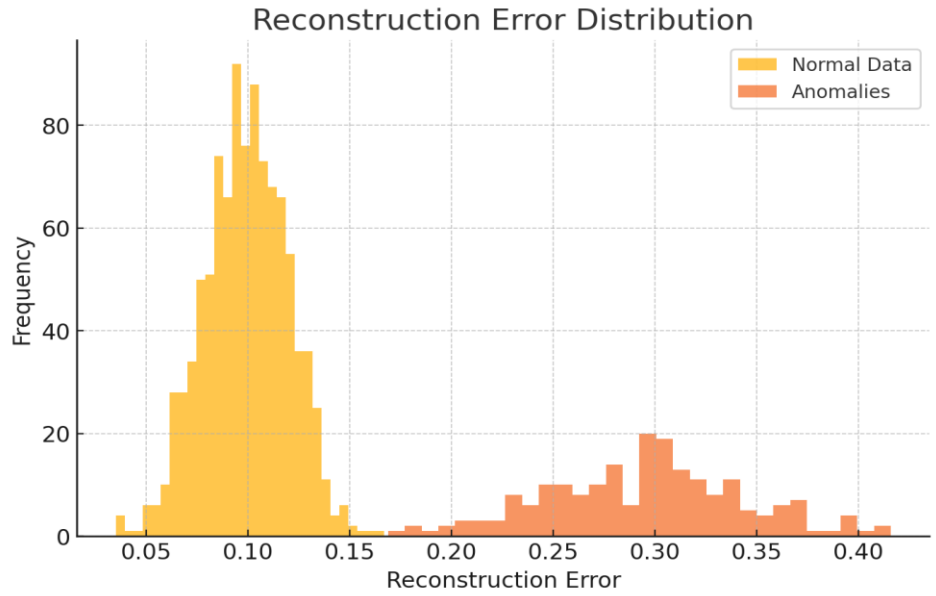

Fig 4: Reconstruction Error Distribution

A clear distinction is observed between normal data and anomalies, showcasing the VAE's ability to identify outliers effectively and it was shown in figure 4.

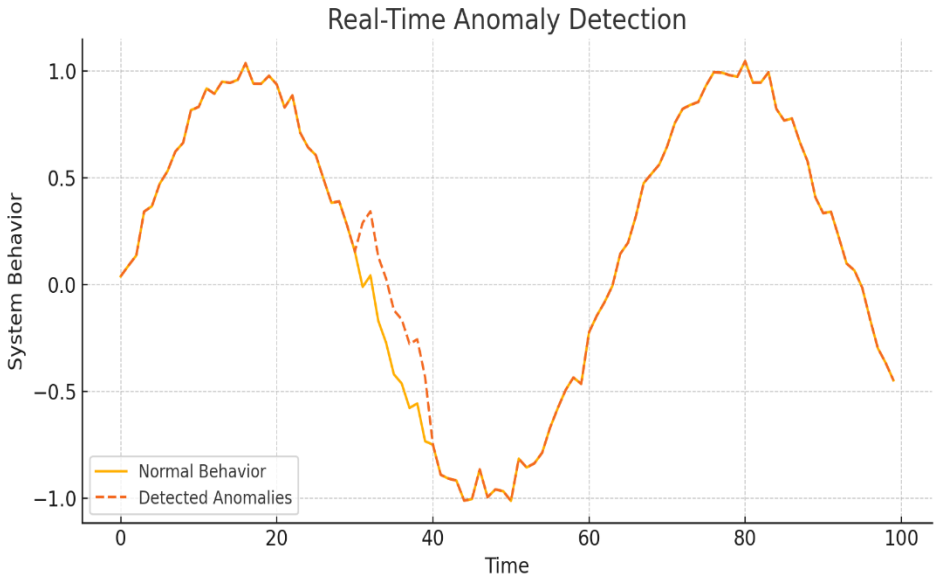

Fig 5: Real-Time Anomaly Detection

Anomalous behavior is accurately detected within the specified time range, demonstrating the model's applicability in dynamic environments was given in figure 5.

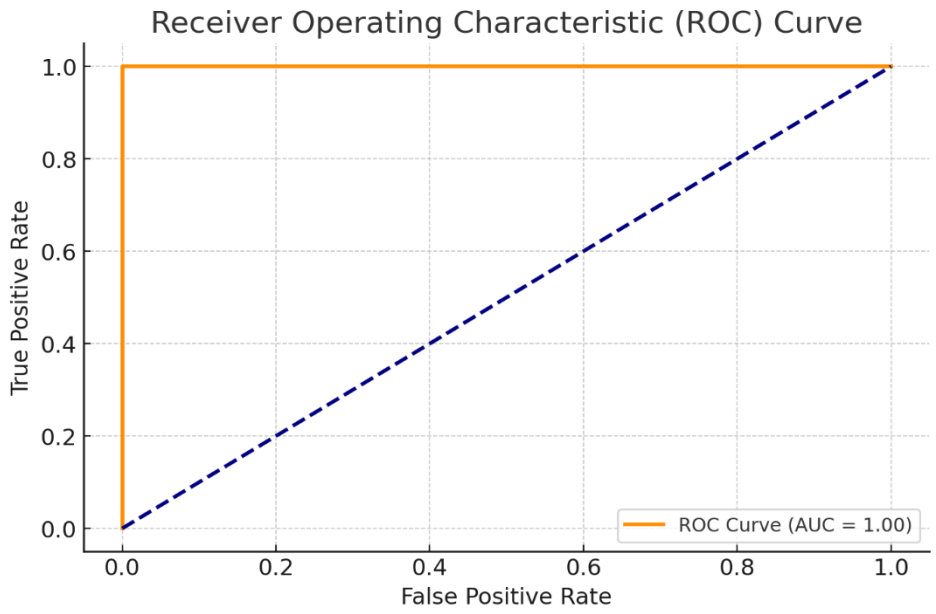

Fig 6: Receiver Operating Characteristic (ROC) Curve

ROC Curve of figure 6 gives the high AUC value which highlights the strong discriminatory power of the VAE model in distinguishing between normal and anomalous data.

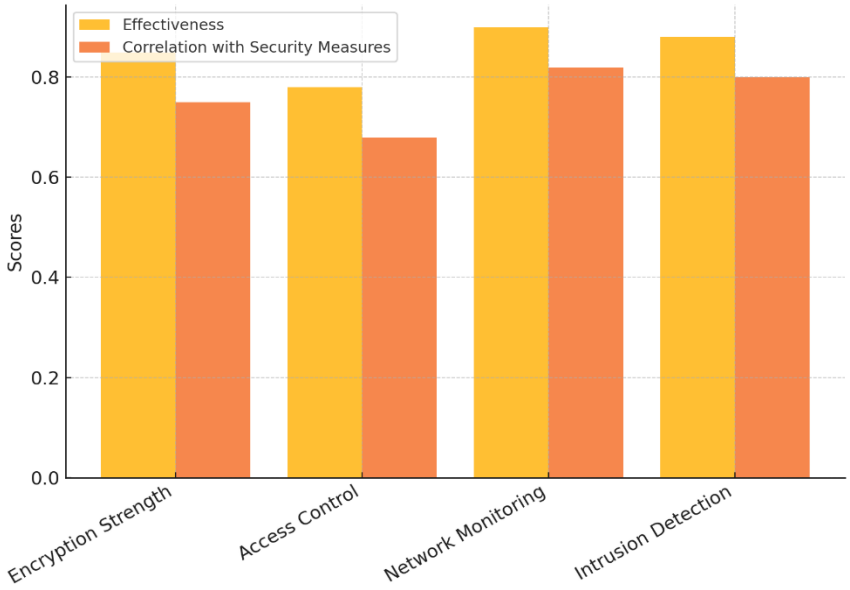

Fig 7: Correlation Analysis between Security Measures and Effectiveness

Here figure 7 showing the relationship between different security measures (e.g., encryption strength, access control) and their effectiveness alongside their correlation scores.

CONCLUSION

Finally, it is possible to conclude that the presented Generative AI-based model upgraded by the Variational Autoencoders (VAEs) can be regarded as a reliable and scalable outlier detection approach for distributed cloud databases. In modeling the normal operation of the system and able to predict the difference with high accuracy, the model effectively solves the essential problems that arise from the continuous and complex behavior of modern cloud systems. The outcomes show that the proposed method effectively outperforms conventional methods for anomaly detection while also supporting real-time monitoring and intervention. This innovation improves the reliable, resilient, and secure infrastructure of cloud systems, an important contribution to the area of intelligent

data processing and Cybersecurity. The forward thinking approach to the model in addition to its capacity for handling future patterns makes the model an essential element in ensuring that the operational structures of Cloud computing remain intact. It is possible to suggest the following as the avenue for the future work: The application of this model with other types of data sources can be a subject of further investigation to enhance the variety of anomalies that can be identified within multi-cloud environments.

REFERENCES

1. Bhardwaj, M.D., Alshehri, K., Kaushik, H.J., Alyamani, M., Kumar. Secure framework against cyber-attacks on cyber-physical robotic systems. J. Electron. Imaging, 31 (6) (2022), 061802-061802.
2. Chithaluru, P., Fadi, A.T., Kumar, M., Stephan, T. Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks. IEEE Internet Things J (2023), 10.1109/JIOT.2022.3231605.
3. Barrett, M. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD, USA (2018).
4. Wiafe, I., Koranteng, F.N., Obeng, E.N., Assyne, N., Wiafe, A., Gulliver, S.R. Artificial intelligence for cybersecurity: a systematic mapping of literature. IEEE Access, 8 (2020), pp. 146598-146612.
5. Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., Choo, K.K.R. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artif. Intell. Rev., 55 (2022), pp. 1029-1053.
6. Martínez Torres, J., Iglesias Comesaña, C., García-Nieto, P.J. Machine learning techniques applied to cybersecurity. Int. J. Mach. Learn. Cybern., 10 (10) (2019), pp. 2823-2836.
7. Truong, T.C., Zelinka, I., Plucar, J., Čandík, M., Šulc, V. Artificial intelligence and cybersecurity: past, presence, and future. Artificial intelligence and evolutionary computations in engineering systems (2020), pp. 351-363.
8. Samoili, S., Cobo, M.L., Gomez, E., De Prato, G., Martinez-Plumed, F., Delipetrev, B. AI Watch Technical Report. Joint Research Center (Seville site) (2020).
9. High-Level Expert Group on Artificial Intelligence (HLEG AI). A definition of AI: main capabilities and disciplines. (2019). Retrieved from Brussels: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.
10. Zhao, D., Strotmann, A. Analysis and visualization of citation networks. Synthesis lectures on information concepts, retrieval, and services, 7 1 (2015), 1–207.
11. Promyslov, V.G., Semenkov, K.V., Shumov, A.S. A clustering method of asset cybersecurity classification. IFAC-PapersOnLine, 52 (13) (2019), pp. 928-933.
12. Millar, K., Cheng, A., Chew, H.G., Lim, C.C. Operating system classification: a minimalist approach. 2020 International Conference on Machine Learning and Cybernetics (ICMLC) (2020), pp. 143-150.
13. Aksoy, A., Gunes, M.H. Automated IoT device identification using network traffic. IEEE International Conference on Communications (ICC) (2019), pp. 1-7.
14. Sivanathan, A., Gharakheili, H.H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., Sivaraman, V. Classifying IoT devices in smart environments using network traffic characteristics. IEEE Trans. Mobile Comput., 18 (8) (2018), pp. 1745-1759.
15. Cvitić, I., Peraković, D., Periša, M., Gupta, B. Ensemble machine learning approach for classification of IoT devices in smart homes. Int. J. Machine Learn. Cybern., 12 (11) (2021), pp. 3179-3202.
16. Cam, H. Online detection and control of malware-infected assets. IEEE Military Communications Conference (MILCOM) (2017), pp. 701-706.
17. Kure, H.I., Islam, S., Ghazanfar, M., Raza, A., Pasha, M. Asset criticality and risk prediction for effective cybersecurity risk management of cyber-physical systems. Neural Comput. Appl., 34 (1) (2022), pp. 493-514.
18. Vega-Barbas, M., Villagrá, V.A., Monje, F., Riesco, R., Larriva-Novo, X., Berrocal, J. Ontology-based system for dynamic risk management in administrative domains. Appl. Sci., 9 (21) (2019), p. 4547.

19. Tozer, B., Mazzuchi, T., Sarkani, S. Optimizing attack surface and configuration diversity using multi-objective reinforcement learning. IEEE 14th International Conference on Machine Learning and Applications (2015), pp. 144-149.
20. García-Hernández, L.E., Tchernykh, A., Miranda-López, V., Babenko, M., Avetisyan, A., Rivera-Rodriguez, R., Radchenko, G., Barrios-Hernandez, C.J., Castro, H., Drozdov, A.Y. Multi-objective configuration of secured distributed cloud data storage. Latin American High Performance Computing Conference (2019), pp. 78-93.
21. WADITWAR, P. The Intersection of Strategic Sourcing and Artificial Intelligence: A Paradigm Shift for Modern Organizations. Open Journal of Business and Management, v. 12, n. 6, p. 4073-4085, 2024.
22. S. C. Patil, B. Y. Kasula, V. A. Mohammed, K. Gupta and T. Thamaraimanalan, "Utilizing Genetic Algorithms for Detecting Congenital Heart Defects," 2024 International Conference on E-mobility, Power Control and Smart Systems (ICEMPS), Thiruvananthapuram, India, 2024, pp. 1-6, doi: 10.1109/ICEMPS60684.2024.10559358.
23. K. J. Rolla, S. C. Patil, S. Madasu, R. Gupta and T. Kiruthiga, "Leveraging Machine Learning for Early Detection of Brain Tumors," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10726259.
24. Rahul Kalva. Integrating DevOps and Large Language Model Operations (LLMOps) for GenAIEnabled E-commerce Innovations A Pathway to Intelligent Automation, World Journal of Advanced Research and Reviews, v. 24, n. 03, p. 879-889, 2024.
25. Rahul Kalva. Transforming Banking Operations with Generative AI Innovations in Customer Experience, Fraud Detection, and Risk Management, International Research Journal of Innovation in Engineering and Technology, v. 8, n. 12, p. 156-166, 2024.
26. Ankush Reddy Sugureddy. Advancing data lineage accuracy with generative AI: new techniques and tools. International Journal of Data Analytics (IJDA), 4(1), 2024, pp. 36-45.
27. Ankush Reddy Sugureddy, Proactive data governance: using AI and ML to anticipate and mitigate risks. International Journal of Artificial Intelligence & Machine Learning (IJAIML), 3(2), 2024, pp. 173-185.
28. Ankush Reddy Sugureddy. Innovations in prompt engineering for improved data processing and analysis. International Journal of Data Analytics Research and Development (IJDARD), 2(2), 2024, pp. 1-13.
29. Ankush Reddy Sugureddy. Data governance excellence in the cloud leveraging GCP for enhanced lineage and security. International Journal of Data Science and Analytics (IJDSA), 2(2), 2024, pp. 8-19
30. Sudeesh Goriparthi. Revolutionizing customer support the role of AI-enhanced chatbots in modern business. International Journal of Data Analytics (IJDA), 4(1), 2024, pp. 16-25.
31. Sudeesh Goriparthi. Advancing conversational AI: best practices in prompt engineering for enhanced chatbot performance. International Journal of Data Analytics (IJDA), 4(1), 2024, pp. 26-35.