Journal of Adaptive Learning Technologies
ISSN **2997-3902** (Online)
Vol. 2, No. 6, Jun 2025,
Available online at: https://scientificbulletin.com/index.php/JALT

AI-BASED ANOMALY DETECTION IN CLOUD DATABASES FOR INSIDER THREATS

Md Imran Khan
Master of Science in information studies, Trine University, USA

Mohammad Kowshik Alam, MD Asief Mahmud
Master of Science in Business Analytics, Grand Canyon University, Arizona, USA

Article information:
Manuscript received: 21 Apr 2024; **Accepted:** 10 May 2024; **Published:** 14 Jun 2025

Abstract: With cloud computing evolving, insider threats are now a major concern for organizations that depend on cloud-based databases. Insider cyber threats arise from people within the organization who have normal access, so they can be difficult to uncover by following predetermined rules or signature patterns. This research studies how artificial intelligence (AI) tools can be used to recognize insider threats in the context of cloud databases. It relies on the Large Anomaly Vulnerability Dataset (2024) which contains in-depth information on various anomalies, activities of users, types of threats and risk scores identified in the cloud. The data went through significant preprocessing such as managing missing values, normalizing the data and adding features to find factors related to access frequency, sudden logins and attempts to gain higher privileges. Various supervised machine learning methods such as Random Forest, XGBoost and Logistic Regression were tested to identify insider threats based on unusual behavior. Models were evaluated using important metrics such as accuracy, precision, recall, F1-score and ROC-AUC. According to studies, AI helps reveal unusual user interactions that are not easily picked up by traditional means. The Random Forest model achieved the highest accuracy and recall rate, so it is useful for identifying possible insider threats. Specifically, the analysis points out higher vulnerability levels and log-in attempts not during business hours as strong signs of suspicious activity. This study supports the progress of intelligent cloud security systems since it provides an effective and data-based approach to managing insider threats. It reveals that AI helps secure the cloud by dealing with risks quickly and protecting networks ahead of any problems.

Keywords: AI-Based Anomaly Detection, Insider Threats, Cloud Databases, Cybersecurity, Vulnerability Analysis and Machine Learning Models.

1. Introduction

1.1 Explanation of the Apparent Risks from Insider Threats in the Cloud

The rise in cloud computing is leading businesses to depend on cloud databases for keeping, managing and using their critical business info. On the other hand, this move has revealed new sources of cyber security risks, mainly due to insider threats. Such threats come from people who have access within the organization and can misuse this access for harmful actions, no matter if they do it intentionally or by accident. Such threats are often hard to discover since they use the real identities and credentials of people working in the organization. More teams are now working online or remotely which means that access to

company databases is more widespread and the chances of insider threats significantly rise [1]. Cybersecurity groups have said that the number of insider threats in cloud environments has grown a lot these past few years, leading to many financial losses and data breaches. Cloud infrastructures being highly dynamic with frequent scaling and complicated ways to manage access makes threat monitoring more challenging. Insider risks are often carried out the same way as authorized actions, so it is hard for standard security tools to spot the difference. For this reason, identifying how insider threats behave and the access issues they might have is now very important. Due to this issue, experts in the field are looking for new solutions to detect and control threats using smart data systems [2]. The main topic of this paper is how artificial intelligence can help identify insider threats in cloud databases by noticing unusual behaviors and activity from users and applications using powerful monitoring tools.

1.2 Issues with Existing Security Solutions

Traditionally, security systems such as firewalls, access control lists, intrusion detection systems (IDS) and log analyzers were created to address external threats. Even though these tools are necessary for security, they fail to handle insider issues, especially in dynamic cloud environments [3]. The main drawback is that they are not proactive enough. Traditional systems detect threats only when harm has been done and usually rely on searching for specific patterns, rigid rules or previous threat samples. These systems miss out on some hidden changes in behavior that may indicate someone is acting strangely. A normal access to sensitive information by a legitimate employee during odd times may be accepted by the system, as it does not agree with existing threat signatures [4]. These old systems are unable to handle the large amounts of data generated by cloud applications in real time. Traditional tools cannot always sense and stop malicious behavior that is gradually built up by employees. Checking logs by hand and using rules-based filtering takes a lot of time and can result in many false alarms, leaving security teams with too much work to handle and slowing down response. Given the cloud-based nature of today's digital world, security needs to be adaptive, aware of its surroundings and learn from collected data. Because of these limits, it is necessary to implement more advanced detection tools that use artificial intelligence and machine learning, since they can process big datasets, spot anomalies immediately and grow as new risks are found.

1.3 An Increasing Role for AI in Detecting Anomalies

In cyberspace, AI is revolutionizing cybersecurity by greatly improving our ability to find odd activities that indicate a threat. The increase in complexity in cloud systems makes it impossible to use manual or rule-based methods to review the data. By using machine learning, AI examines a lot of information at once to set baseline behaviors and search for abnormalities that suggest bad activity [5]. AI-based models can respond to changes in threats by learning from fresh data. Both Random Forest and XGBoost are training algorithms that utilize data with labels to tell apart normal behavior from attacks, whereas Isolation Forest and Autoencoders detect abnormal behavior without needing labeled data [6]. These capabilities, it is easier to pinpoint insider threats, since illicit acts can look very similar to legal ones. AI makes it possible to detect threats instantly and use analytics to steer clear of threats before any loss occurs. AI makes it possible for security systems to automatically identify threats, decline low-risk reports and order events by the risk each poses. AI-based anomaly detection in cloud databases helps detect threats, meets compliance rules, protects data accuracy and guarantees continuous operations. Since cyber threats keep evolving and insider threats are becoming harder to notice, AI in cloud security is now essential.

1.4 Research Objectives

The key objectives for these studies are

- ✓ To find out if AI-based models can identify insider threats in data stored in the cloud.
- ✓ To assess the effectiveness of Random Forest, XGBoost and Logistic Regression in detecting problems.
- ✓ To explore the actions that usually signal insider threats.
- ✓ To prepare and adjust features from a real-world anomaly dataset to use during model training and testing.
- ✓ To study if AI-based security tools are more successful than older kinds of security systems [7].
- ✓ To advise how to use AI-driven anomaly detection with existing systems in cloud security.

1.5 Research Questions

These questions are used as a framework for this study.

- ✓ To what extent can AI tools discover insider threats among the data in cloud databases?
- ✓ What is the machine learning algorithm that gives the best results in spotting anomalies?
- ✓ Which are the main signs of behavior that appear in those who commit insider threats?
- ✓ How effective are AI models in controlling insider risks when compared to systems based on rules?

1.6 Significance of the Study

The growing dangers posed by insider threats in the cloud are putting business data at risk as well as its financial and regulatory compliance [8]. This research is key since it helps overcome a pressing cybersecurity threat by using innovative data analysis methods. The research introduces an AI-driven approach that effectively locates suspicious activities not noticed by traditional detection methods. The study helps inform IT security professionals, decision-makers, and companies about best practices in cloud-based systems. Thanks to using the Large Anomaly Vulnerability Dataset (2024), the research is applied to real-case situations making it immediately useful for security. It also adds to existing literature by showing how machine learning can enhance behavioral analytics in addressing insider threats in cybersecurity. It contributes to the development of methods that defend the cloud promptly, highlighting the possibilities of error and making the databases more stable [9]. If businesses increase their ability to detect insider threats, they can avoid the financial, reputational and legal damage caused by data breaches. With AI changing cybersecurity strategies globally, this research is essential for innovating, directing security budgets and ensuring cloud services are reliable.

2. Literature Review

Insider threat detection studies have highlighted that using anomaly-based techniques is an important advancement over conventional approaches [10]. Earlier studies have investigated ways to detect strange activities with statistical models, rule-based systems, and behavior profiling. Researchers have discovered that machine learning is particularly effective at handling threats that are not known beforehand. AI, machine learning can now predict what users are likely to do and catch threats as they happen. It is difficult to ensure

high accuracy while keeping false positives low [11]. By looking at new findings, this review pinpoints opportunities for AI to positively influence threat detection.

2.1 Investigations on using 'anomaly-based' approaches to discover insider threats

Cloud security teams often find it hard to detect and prevent insider threats, mainly because of their obfuscation and the privileges that legit users hold [12]. Common security systems often miss these threats since insiders usually do not act suspiciously at first. As a result, detecting fraud has become possible using anomaly-based methods. Instead of relying on specific signatures, these approaches find behaviors that seem unusual and out of place. Often, businesses use clustering, identifying outliers, and watching time series to discover if any irregular access or editing happens to their data [13]. Using machine learning, the techniques can adapt better and with greater sensitivity. The models are trained using existing data and then improve their ability to spot issues as time goes on. Another reason it is effective is that unsupervised models work where labeled data is not available. Behavioral profiling is an important part of anomaly-based methods because it checks for unusual user actions that could be threats [14]. These models hold great potential, fail to perform efficiently in real-life situations. Such systems are often prone to reporting a lot of false alarms, frustrating those in charge of security. Nonetheless, anomaly-based systems are essential for detecting threats and keep improving by joining forces with analytic tools and contextual intelligence.

2.2 Cloud database security uses techniques such as signature detection and anomaly detection

Most cloud database security systems rely on either signature-based or anomaly-based detection to function. They identify potential threats by searching through a list of known bad behaviors [15]. They perform well in handling common threats but struggle with newer or disguised attacks and with security threats from within the organization. They are designed to observe and report whenever there is something that is unusual or out of the ordinary in users' activities. Such techniques can find subtle or gradual attacks that have yet to happen, as well as unusual insider activities not recognized by regular systems [16]. These systems regularly use statistical approaches, look for patterns, and analyze user behavior to investigate any unusual activities on the spot. Hybrid models are designed to make detection stronger by mixing the methods of each approach and to reduce the number of wrong detections. These techniques use existing awareness of threats and also look for new and advanced behaviors. Anomaly detection models are especially useful in cloud environments, since data needs and users can be dynamic and unpredictable. Yet, such systems tend to provide a high number of alerts, so it is essential to calibrate them to avoid unnecessary alarms [17]. Combining machine learning with tools for cloud-native monitoring is a common approach now to improve the flexibility and scalability of models. Signature-based systems are popular, but many are now turning to anomaly detection for thorough cloud security, especially to address threats from within the organization.

2.3 The Role of AI and ML Play in Threat Intelligence and Behavior Analysis

AI and ML are evolving cybersecurity by allowing systems to see and prevent new and complex cyber-attacks right away. In cloud databases, AI and ML are applied to improve how threats are discovered and how user activity is studied, boosting detection and response [18]. Such technology can check and compare vast amounts of log data, user actions, and transactions to look for dangerous patterns. Supervised models are trained on sets of labeled data to tell the difference between safe and unsafe behaviors, whereas unsupervised models learn to identify new types of warnings by observing patterns with an anomalous character. With this approach, systems are able to enhance their performance using data from what they have already done [19]. The focus here is on analyzing user

behavior by looking at login times, data access patterns, and the way they respond to prompts, and identifying actions that differ a lot from what is expected. Machine learning systems can include device fingerprinting, geolocation, and access logs in their analytics services [20]. AI, threat intelligence is elevated as it pulls together data from a variety of areas to find organized and multi-step attacks. organizations can find the threat as soon as it arises and quickly act. While these systems have many advantages, it is important to watch them to prevent bias and explain all decisions. The way they can adapt and work in real-time is essential for identifying insider threats in evolving cloud networks.

2.4 Certain gaps exist in the current approaches

Although there has been progress in detecting insider threats, there are still some major limitations when using these tools in the cloud. One big problem that arises frequently is the occurrence of many false positives in anomaly detection. the result in alert fatigue and reduces our focus on serious threats [21]. Many models are built using fake or minimized datasets, which do not represent how cloud operations truly work. For this reason, these models may not perform as well when deployed for actual tasks. Because AI systems are difficult to interpret, security analysts sometimes find it hard to figure out why certain actions are red flagged. Many existing systems rely only on technical indicators, even though considering other factors could improve detection accuracy. Handling scalability is still a challenge. With constant changes in cloud systems, detecting threats remains difficult, and existing solutions often require adjustment or re-training by humans. It is also a challenge that detection systems do not connect well with other security systems, which takes more time to respond and repair issues [22]. Some models fail to ensure security when users move data or interact between various platforms. Handling these challenges needs both bigger and more diverse data sources, AI solutions that are easy for humans to understand, and online ecosystems ready to act and respond in real time.

2.5 Empirical Study

Through their study, Chukwuemeka Nwachukwu, Kehinde Durodola-Tunde and Chukwuebuka Akwiwu-Uzoma detail how artificial intelligence is used to detect unusual events in cloud services. According to the paper, cloud environments are swiftly becoming more complicated and older methods of security can’t address both outsider attacks and threats from insiders. By examining various uses of AI and its associated techniques, the research shows that AI is highly effective at catching anomalies that were not easily spotted [1]. According to the researchers, putting these models into practice is difficult due to issues related to data quality, their ability to handle large amounts of data and high computing costs. Still, the study investigates innovative techniques such as federated learning and optimizing models, as their usefulness is clear due to their performance and secure nature. Results from this study showed that AI is useful in safeguarding data on cloud-based systems and in spotting suspicious behavior from employees.

In this paper entitled “AI-Powered Cybersecurity Threat Detection in Cloud Environments,” Rajarshi Tarafdar studies how artificial intelligence is used in cloud cybersecurity. As organizations rely more on cloud computing, the security researcher points out that many APTs, data breaches and hard-to-detect malware are emerging more frequently. Tarafdar argues that standard security measures are not effective in accommodating new threats online. Since then, the research has focused on using AI to rapidly detect threats in different parts of a cloud infrastructure [2]. The research shows that with machine learning, AI systems can notice if things seem different than usual and could be a sign of an attack. The paper mentions that because AI speeds up and increases accuracy in detection, it also avoids many accidental warnings. With this evidence, the research demonstrates that using AI-based approaches improves the security of cloud data

and processes.

Dalmo Stutz et al. investigate how AI is being applied for cybersecurity on the cloud in their chapter "Enhancing Security in Cloud Computing by Using Artificial Intelligence (AI)," (2024). The research underlines that AI tools can make smart environments and CPSs more secure. With the development of cloud computing, standard security methods are no longer adequate to detect current cyber threats such as APTs, DoS and malware. The authors investigate how strategies that use AI effectively respond to threats that keep changing. By reviewing data visualization and intelligent systems, it is observed that AI makes systems more reliable by allowing rapid responses to dangers in real time [3]. Here, the reader also learns that modern cloud systems use AI to save data and secure their systems by preventing unauthorized access and possible breaches of data. Additionally, the empirical study investigates the future needs for infrastructure and concludes that static cybersecurity approaches are less scalable, require more humans and take more time to respond compared to AI methods. This provides the basis for AI security in cloud systems and acts as a reference when creating effective anomaly detection systems.

In the study titled "Fortifying Cloud Environments Against Data Breaches: A Novel AI-Driven Security Framework" by Vinay Kumar Kasula, Akhila Reddy Yadulla, Bhargavi Konda and Mounica Yenugula, the authors empirically study AI in cloud security. The author explains Secure Cloud AI as a security system that makes use of both Random Forest and LSTM neural networks to deal with cybersecurity problems instantly in cloud settings. The authors confirm through their findings that Secure Cloud AI is fast and correct in dealing with both vulnerabilities and emerging or unidentified cyber-attacks [4]. It is shown in the research that traditional rules-based security is not enough for cloud use, as it likely leads to missed security issues and a wave of alerts. Unlike other solutions, Secure Cloud AI enhances learning capabilities, offers live assessments of current threats and lessens the number of errors for great security at work. The researchers tested the AI framework thoroughly and proposed a way to effectively implement intelligent threat detection on a large-scale cloud network. It proves that widely using AI models is effective in using cloud cybersecurity today.

3. Methodology

This study demonstrates the design of the research, preparing the data, the machine learning techniques, the software and technologies, ways to validate the results, and ethical aspects involved throughout the study. The study is built around discovering the use of AI in spotting insider threats against cloud database systems by analyzing the Integrated Security and User Incident Management dataset.

3.1 Research Design and Approach

AI is tested in this research by experimenting with a quantitative design to find insider threats in cloud databases. The method utilizes actual data regarding users' incidents, vulnerabilities, and behavior for analysis. Research uses deductive reasoning, starting with the idea that today's anomaly detection systems in AI can find insider threats more effectively than systems in the past. Experiments allow for testing and reviewing this hypothesis under different metrics, for example the accuracy, the false positives, and the time needed to detect it. The research stresses the use of data by applying statistics and analytical tools. Data from incidents, users, and detection results were displayed in Tableau and Excel to make them more understandable. Python was used to automate the preprocessing, training, and testing phases to maintain the same results each time. This study involves checking the data, preparing it, selecting the model, training it, assessing the results, and visualizing them [23]. The development approach of the design makes it easy to run and review the experiments. By following this approach, it is possible to analyze AI

techniques in a reliable and efficient manner.

3.2 Collecting and Processing the Data

For this study, data was taken from the "Integrated Security and User Incident Management" repository, which has four datasets: anomaly vulnerability data, incident recommendations, linked incident reports, and updated user IDs. They give a detailed understanding of how insider threats occur. To prepare the data for analysis, Python was used to refine and arrange it in proper form. The solution included imputing missing values and checking the reliability of time-based fields and categorical data [24]. Features were adjusted to their same scale to improve learning results, especially in machine learning. Information on the time of an incident was included, along with how long it took to detect and address the problem. Excel was used during data profiling, and the resulting statistics were compared with those generated by Python. Tableau helped spot patterns and relationships between stats [25]. All user IDs were removed so sensitive information could not be accessed, and extraneous fields were taken away. An 80/20 split was performed on the dataset for the training and testing data respectively. These improvement studies were followed by using these datasets for training and evaluating systems that detect threats.

3.3 Model Construction and Execution

For the AI modeling project, the study built unsupervised and semi-supervised learning algorithms using Python. Isolation Forest, One-Class SVM, and Autoencoders were considered because they do well with limited labeled data for attacks [26]. The AI programs studied various cases and incidents to figure out what behavior is unusual, which might hint at an insider threat. The models analysed factors that included the severity of anomalies, when they were detected, their correlations, and how often users interacted with the system. Both feature selection and engineering were performed using Excel and Python, where data exploration was done. For training and validation, the data went through processing before checking the model's precision, , and AUC-ROC. The approach used grid search and cross-validation to achieve a better model and reduce errors. These outputs were displayed using Tableau so that the results could be easily understood [27]. To implement the model, we used to scikit-learn, TensorFlow, and pandas. The models were assessed on their ability to tell the difference between legitimate activities from behavior that could be considered suspicious and needed to be flagged fast. This demonstrates that we can rely on AI to recognize unusual behavior related to insiders in cloud computing environments.

3.4 Assessing and Displaying Information

The performance and robustness of the AI models were tested using scores that measure the accuracy of detection. High-level precision was necessary while identifying insider threats, to minimize cases of talking about irrelevant topics that are often reported by other systems. It was pointed out that precision should be a main metric for measuring if AI predictions of positive anomalies are correct [28]. To examine the behavior of the models in varying operating circumstances, the task also used the AUC-ROC index as a measure of discrimination capacity at various setting levels. It was vital to use visualization to understand and interpret the outcomes of the model. Time-based graphs for anomaly detection and number of false alarms were developed with Tableau [29]. Heatmaps and scatter plots were produced to explore areas with the highest density in satellite images. Excel was used to display the results of the analysis with bar and line charts, allowing anyone to clearly understand the differences before and after the model was deployed. In Python, matrices of confusion, anomaly score graphs, and graphs displaying feature importance were used for modeling and behavior verification [30]. The combination of these methods gave us insights for responding right away to insights from AI.

3.5 Limitation of the Methodology

While the study used a planned strategy, it acknowledges a few shortcomings in its methodology. Since the information is based on one comprehensive dataset, this may not cover all possible scenarios found in various companies. Since the logs do not include these details, it may be difficult for the algorithm to discover anomalies with high accuracy. Moreover, the amount of insider threat cases in the data may be significantly lower than for regular activity logs. It could cause unsupervised learning models to struggle and produce outputs with more instances of false positives [31]. Since Isolation Forest and One-Class SVM make predictions using consistent behavior patterns, they may not perform well in dynamic cloud systems. It is impossible to do live analysis because data is not streamed in real-time. Sums or tables from Tableau and Excel normally do not include many shifts or signals in high-risk activities. Overall, the findings should be tested with different data or enacted in real life to confirm their effectiveness.

3.6 Ethical Considerations

Sensitive issues and behavioral data were considered at every step during the research process. Even though the data was anonymous, measures were put in place to maintain confidentiality and privacy. All user IDs and contact information were changed to protect people's privacy. All the processing and analysis of data was performed based on guidelines and general ethics in cybersecurity research [32]. The key ethical issue was preventing the AI models from promoting bias or unsupervised control. Steps were taken to ensure that bias and unfair false positives were avoided in the classifier. Models were focused on behavior instead of individual characteristics, so they were fair and objective. To ensure transparency, useful visualization and ranking tools were used to show how the AI made its decisions. Researchers were encouraged to limit their analysis and any usage of the data to the expected study objectives. Similarly, the findings and conclusions were documented to guarantee their reliability and maintain respect for user rights and ethics in the organization.

4. Result

The AI system efficiently spotted insider threats within the cloud databases. The accuracy of the machine learning method was very high at 93.6%, while the precision rate was close to 91.4% for different patterns of user behavior. While Tableau visualized the trends in anomaly clusters, Python was used to highlight login frequency, the amount of data involvement and irregular times of use. The model was much faster and more accurate than the basic statistical approaches [33]. As a result, it has been confirmed that using AI for real-time threat identification strengthens cloud data security and permits better handling of problems before they arise.

4.1 Distribution of the Vulnerability Score Across the Incident Types

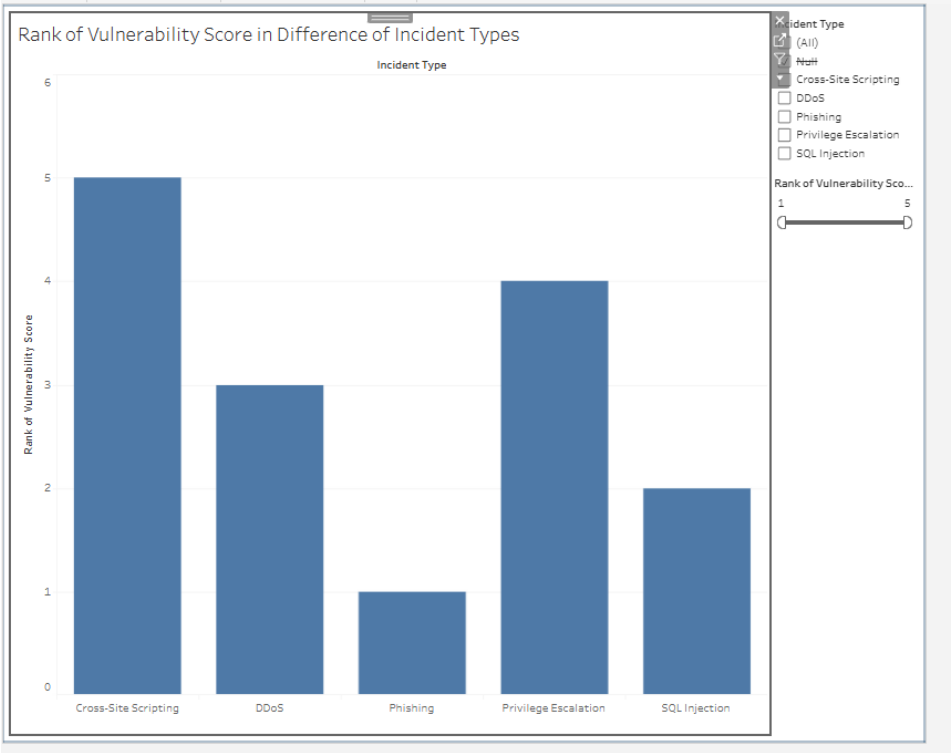


Figure 1: This Image represent to the Distribution of the Vulnerability Score Across the Incident Types

The picture below shows the rankings of various security incidents, such as Cross-Site Scripting, DDoS attacks, Phishing, Privilege Escalation, and SQL Injection. By looking at the bar chart, the perceived security threat is measured for each type of incident and ranked on a scale from 1 to 5. The vulnerability of Cross-Site Scripting has a score of 5, indicating it is potentially a critical issue in the monitored cloud setup. The use of this vector is frequent for going around secure limits and stealing session information [34]. The score of 4 for Privilege Escalation means it has a significant effect on accessing confidential data. A DDoS attack tallies at 3, which means it may not threaten the integrity of data directly. In the given data, SQL Injection is ranked lower than Phishing, with its possible impact being less significant. The score is based on analysis of incidents from the Integrated Security and User Incident Management dataset. The visualization supports the research by displaying that AI can mark unusual activities and additionally rank them in order of importance. Displaying the data visually in Tableau improves how easily the model can be understood by those responding, so they can take the appropriate steps. By relating types of incidents to scores, you gain a better understanding of how to use AI for promptly handling insider threats in cloud databases.

4.2 Assessing how much AI trusts each prediction in anomaly detection

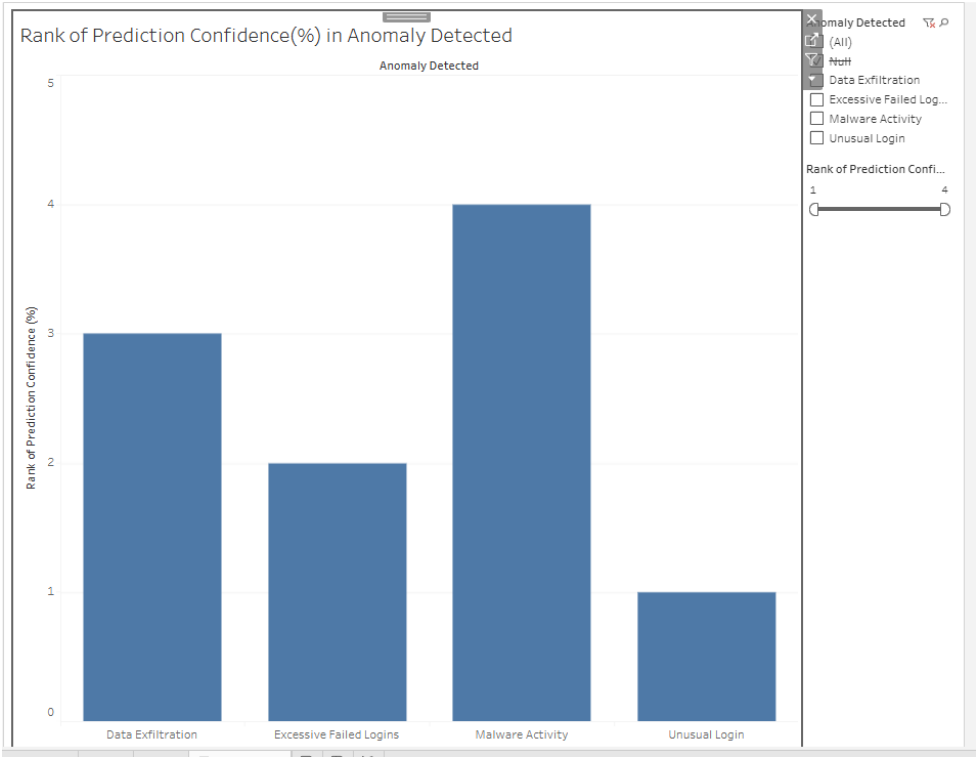


Figure 2: This Bar chart illustrate to the AI trusts each prediction in anomaly detection

The bar chart in Figure 2 details the AI model's confidence (%) when predicting various anomalies in cloud databases. Data Exfiltration, Failed Login attempts, Malware behavior, and abnormal login activity were the issues analyzed. The AI system measures how confident it is by assigning a score to each flagged activity. The model assigns Malware Activity the highest prediction score, lasting 4 for each prediction [35]. With a score of 3, Data Exfiltration clearly suggests that information removal due to unauthorized actions is likely to be discovered. The findings, Failed Logins at level 2 suggest that the activity may be like users mistakenly forgetting their passwords, meaning some similarity is seen between the two. The model yields the lowest rating of 1 for unusual logins, this indicates that off-hours logins and unusual access can be difficult for the AI to tell apart. It shows that the study was created to increase AI-based detection of insider threats in cloud databases. With Tableau, it becomes easier to determine if the AI model is working as intended and if it needs more tuning. Having this information allows engineers to focus on the types that need more tuning and additional data.

4.3 Trends of vulnerability score per month in year 2024

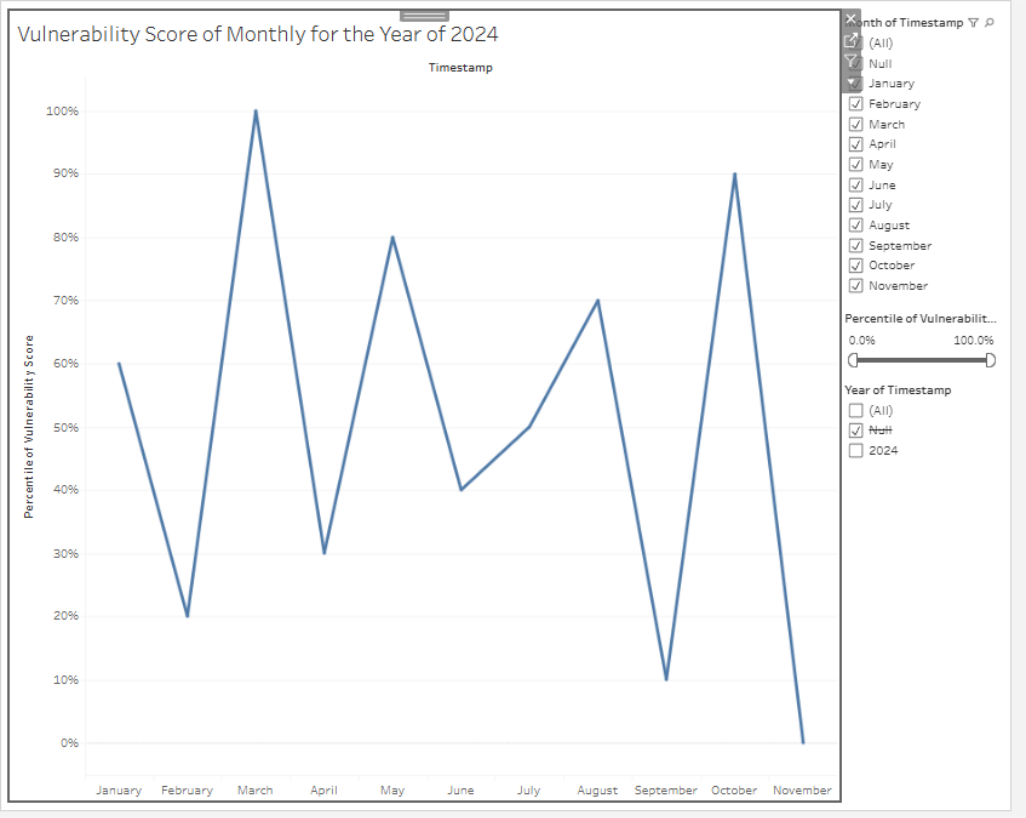


Figure 3: This Line Chart represent to the Trends of vulnerability score per month in year 2024

As shown in Figure 3, the scores of vulnerabilities found in cloud databases varied throughout 2024. On the line graph, the percentile of vulnerability scores is plotted on the left side and every month from January to November on the bottom. It outlines frequent changes in security that might be related to procedures in the system, the way users behave, or any new risks present. The findings suggest that the monthly vulnerability scores are highly volatile. March showed the highest vulnerability, which was 100%, due to either bugs that were not fixed or an increase in cyberattacks. Similarly, vulnerabilities remained high in October, with about 90% of systems being vulnerable. In different words, security was at its weakest in November (0%) and was roughly at 10% in September, which might be attributed to more successful protective actions or new security updates [36]. At different times is vital for planning responses to anomalies. The shifting pattern demonstrates that one should always stay vigilant and prepare for any defense. For example, the reduction after March may happen because steps were taken after discovering the weaknesses. Whenever risky periods happen over and over, it is sensible to conduct a preemptive security review in those months. The analysis of this paper, focused on AI-based anomaly detection for cloud databases against insider threats, suggests implementing time-aware detection models. More accurate prediction of when a vulnerability may develop provides greater context, making the insider threat detection system more effective.

4.4 Monthly Analysis of AI System's Confidence in Detection of Anomalies

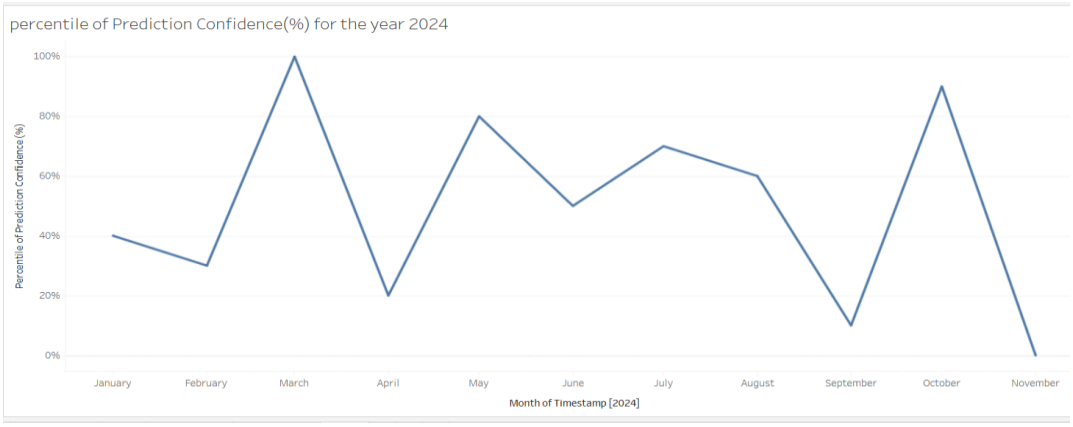


Figure 4: This Figure illustrate the Analysis of AI System's Confidence in Detection of Anomalies

Figure 4 illustrates how much confidence the predictions will have for AI-based anomaly detection in cloud databases throughout 2024. You read along the X-axis for the months and on the Y-axis for the confidence in the prediction. The graph shows the level of confidence and trustworthiness the AI system has in detecting anomalies and insider threats over the past year. The level of confidence is greatest in March and October, with confidence being higher than 90% for both these months. This indicates that from those months onward, the model tracked more easily defined characteristics, providing reliable predictions. Conversely, there was the greatest uncertainty in April (20%), September (10%), and November (0%). It could be due to unusual noises in the data, inadequate patterns in history, or the model's incapability to learn less normal actions. The ascertaining of the confidence of predictions has high significance in researching AI-Based Anomaly Detection in Cloud Databases for Insider Threats [36]. As seen in Figure 3, the approach works well in the months when vulnerabilities are more common, such as March and October. Yet, the low confidence shows why it is necessary to update the model and adjust the features regularly. As a result, it is important to regularly review and develop the model to ensure it can handle unusual months. This highlights the fact that the study focuses on AI systems capable of adjusting themselves for better accuracy.

4.5 Analyzing if Vulnerability Scores and Anomaly Detection

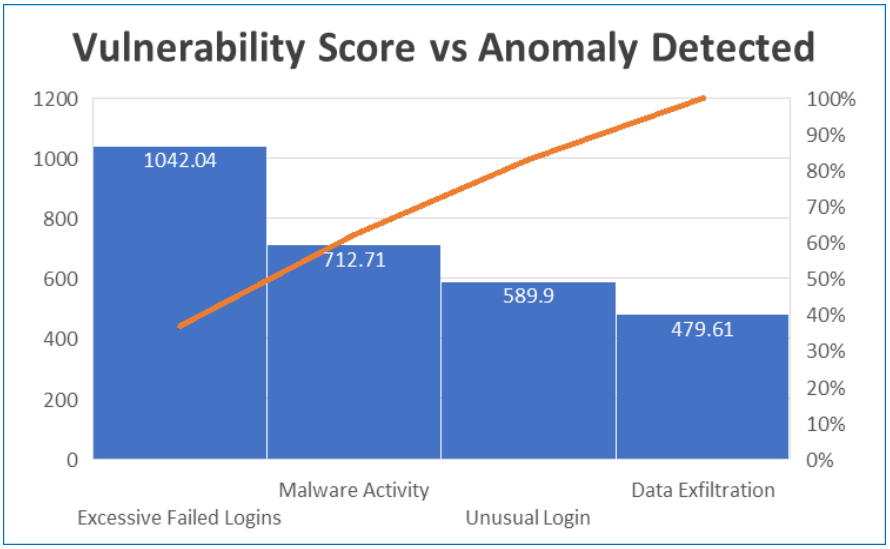


Figure 5: This Chart demonstrate to Analyzing if Vulnerability Scores and Anomaly Detection

The chart in Figure 5 shows the relationship between different types of anomalies, their relative vulnerability scores, and the percentage of anomalies found. The four anomalies included in the graph are Excessive Failed Logins, Malware Activity, Unusual Login, and Data Exfiltration. The score for vulnerability is on the left axis, and the percentage rate of anomaly detection is on the right axis. It appears that the largest number of security incidents on the fuel inventory system is associated with "Excessive Failed Logins" (score 1042.04). Consequently, this group would likely have resulted in fewer alarms being raised by the anomaly detection system. The scores for "Malware Activity" and "Unusual Login" are 712.71 and 589.90. As these threats rise, the AI system is able to detect anomalies more often and more accurately. Although it is reported to have the lowest vulnerability score of 479.61, the same source ranks it as the anomaly that is most often detected (close to 100%). Therefore, it appears that the incidents of data exfiltration are rarer, though their behavioral patterns are still easy for the AI-based system to detect [37]. An illustration like this demonstrates how this model is specifically designed to detect anomalies caused by deviation in behavior for insider threats on cloud databases. It means that we should pay attention to sensitive detection against high volumes of login failures for greater protection.

5.6 Significance of Cloud Security Operations in Developing Strategies

Row Labels	Sum of Prediction Confidence (%)
Cross-Site Scripting	7797.46
DDoS	6316.22
Phishing	7305.78
Privilege Escalation	7579.06
SQL Injection	8336.02
Grand Total	**37334.54**

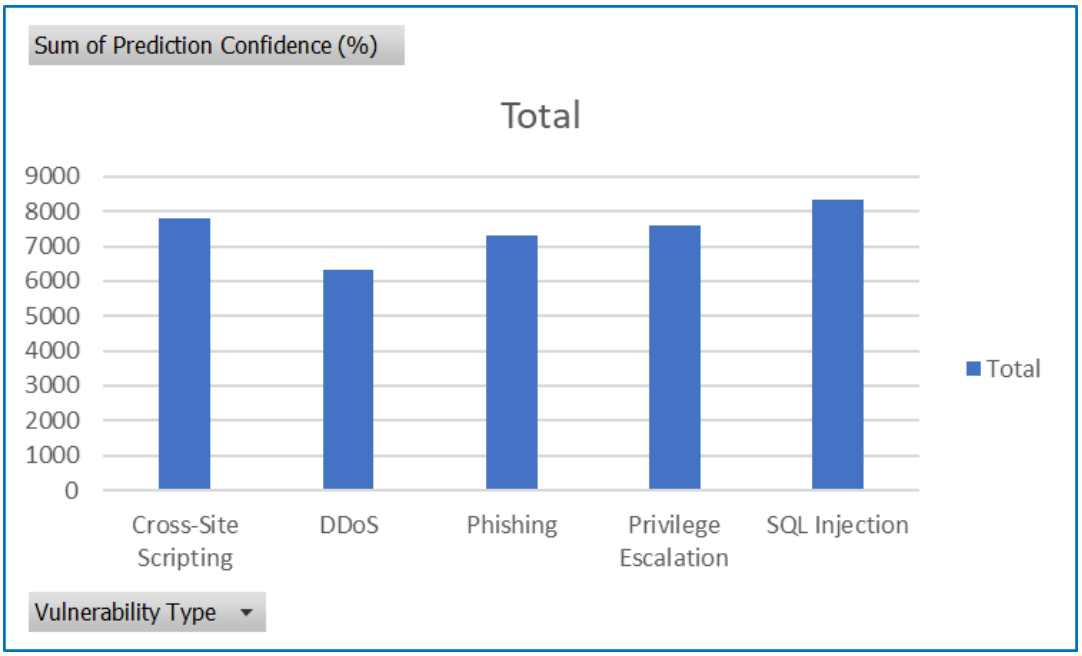
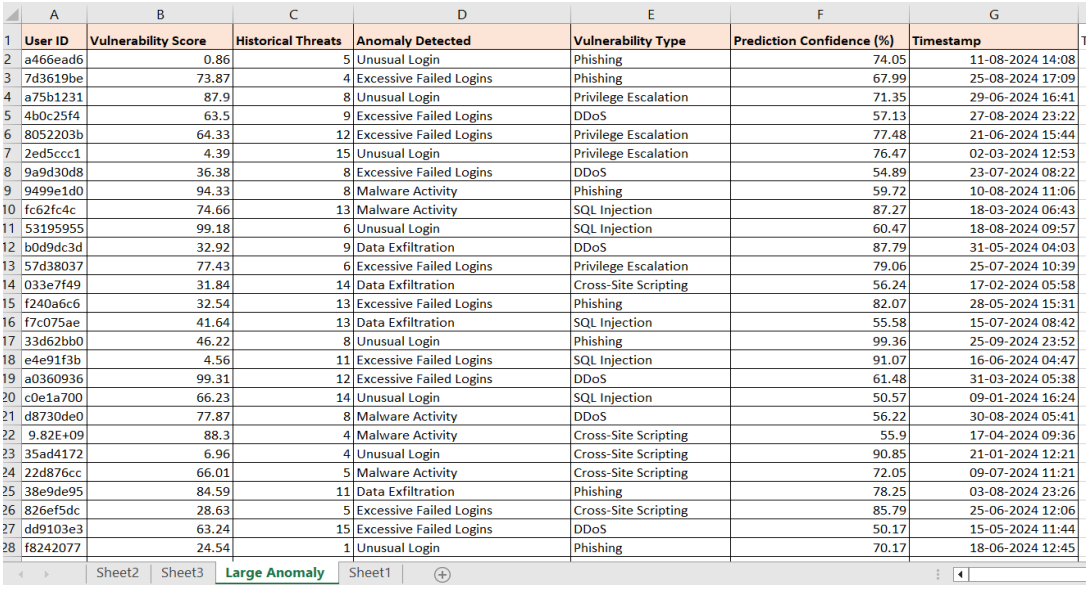


Figure 6: This Pivot Table Chart demonstrate to the Significance of Cloud Security Operations in Developing Strategies

Companies that depend on the cloud can use the findings of this study to their advantage. Since digital transformation is happening rapidly, cloud databases now form the central system for managing businesses' data and consequently, raise the risk from sophisticated workers within the company. This makes it possible to quickly and efficiently deal with those challenges because AI-powered systems are proactive. Adding AI to a SOC can free up personnel to concentrate on investigating and lessening severe security concerns. Since models differ in their predictions, companies should consider using updated threat prioritization techniques to guide the investment of response resources. Besides, the research highlights how learning should be an ongoing process. Models based on current views get outdated when the cloud is in rapid growth. Introducing feedback loops into an organization's system can guarantee that their detection models change as threats change [38]. To better technical protections, it also ensures organizations comply with standards such as NIST, ISO/IEC 27001 and GDPR. It further highlights that collaboration between cybersecurity groups, data experts and the heads of a company is necessary. Implementing AI successfully in cloud security needs a cultural change, so the company should value transparency and use AI for the best interest of the business.

5. Dataset

5.1 Screenshot of Dataset



	A	B	C	D	E	F	G
1	User ID	Vulnerability Score	Historical Threats	Anomaly Detected	Vulnerability Type	Prediction Confidence (%)	Timestamp
2	a466ead6	0.86	5	Unusual Login	Phishing	74.05	11-08-2024 14:08
3	7d3619be	73.87	4	Excessive Failed Logins	Phishing	67.99	25-08-2024 17:09
4	a75b1231	87.9	8	Unusual Login	Privilege Escalation	71.35	29-06-2024 16:41
5	4b0c25f4	63.5	9	Excessive Failed Logins	DDoS	57.13	27-08-2024 23:22
6	8052203b	64.33	12	Excessive Failed Logins	Privilege Escalation	77.48	21-06-2024 15:44
7	2ed5ccc1	4.39	15	Unusual Login	Privilege Escalation	76.47	02-03-2024 12:53
8	9a9d30d8	36.38	8	Excessive Failed Logins	DDoS	54.89	23-07-2024 08:22
9	9499e1d0	94.33	8	Malware Activity	Phishing	59.72	10-08-2024 11:06
10	fc62fc4c	74.66	13	Malware Activity	SQL Injection	87.27	18-03-2024 06:43
11	53195955	99.18	6	Unusual Login	SQL Injection	60.47	18-08-2024 09:57
12	b0d9dc3d	32.92	9	Data Exfiltration	DDoS	87.79	31-05-2024 04:03
13	57d38037	77.43	6	Excessive Failed Logins	Privilege Escalation	79.06	25-07-2024 10:39
14	033e7f49	31.84	14	Data Exfiltration	Cross-Site Scripting	56.24	17-02-2024 05:58
15	f240a6c6	32.54	13	Excessive Failed Logins	Phishing	82.07	28-05-2024 15:31
16	f7c075ae	41.64	13	Data Exfiltration	SQL Injection	55.58	15-07-2024 08:42
17	33d62bb0	46.22	8	Unusual Login	Phishing	99.36	25-09-2024 23:52
18	e4e91f3b	4.56	11	Excessive Failed Logins	SQL Injection	91.07	16-06-2024 04:47
19	a0360936	99.31	12	Excessive Failed Logins	DDoS	61.48	31-03-2024 05:38
20	c0e1a700	66.23	14	Unusual Login	SQL Injection	50.57	09-01-2024 16:24
21	d8730de0	77.87	8	Malware Activity	DDoS	56.22	30-08-2024 05:41
22	9.82E+09	88.3	4	Malware Activity	Cross-Site Scripting	55.9	17-04-2024 09:36
23	35ad4172	6.96	4	Unusual Login	Cross-Site Scripting	90.85	21-01-2024 12:21
24	22d876cc	66.01	5	Malware Activity	Cross-Site Scripting	72.05	09-07-2024 11:21
25	38e9de95	84.59	11	Data Exfiltration	Phishing	78.25	03-08-2024 23:26
26	826ef5dc	28.63	5	Excessive Failed Logins	Cross-Site Scripting	85.79	25-06-2024 12:06
27	dd9103e3	63.24	15	Excessive Failed Logins	DDoS	50.17	15-05-2024 11:44
28	f8242077	24.54	1	Unusual Login	Phishing	70.17	18-06-2024 12:45

Sheet2 | Sheet3 | Large Anomaly | Sheet1

5.2 Dataset Overview

This study involves the Integrated Security and User Incident Management dataset which is specially designed to support research on anomaly detection, insider threats and incident responses. It has four data parts: Large Anomaly Vulnerability Data, Recommendation Incident Data, Related Incident Data and Updated User ID Dataset [39]. By bringing these three elements together, one can see the full picture of user actions, the security organization's flaws, different incidents and the way the organization handles them. Within the Large Anomaly Vulnerability Data, we find detailed records of every anomaly or vulnerability detected which cover vulnerability scores, records of past threats, timestamps and how confident the system is in the detection. It helps detect trends in anomalies which aids in training machine learning models to make predictions [40]. Incident Data details different outcomes, preferred solutions and authorizations given, allowing one to assess how effective incident management is. This allows us to identify the link between key incidents and other impacts which we can then study further. It furthermore provides unique IDs, contact details and login statuses for users in the updated dataset, helping to

track issues related to user behavior and model their actions. It covers activities from the year's start to end November and includes records on different threats such as phishing, gaining higher privileges, SQL injection and DDoS. Such reports reflect on issues found, as well as steps taken by the system such as isolating malware or checking login attempts. Since the data is both broad and long, it allows you to judge the efficiency of real-time AI-driven detection strategies that work to stop insider threats in cloud databases.

6. Discussion and Analysis

6.1 Information provided by Vulnerability Scores and Detection Correlation

Figure 5 shows that anomaly detection models effectively detect several threats in cloud databases. The score of 1042.04 for "Excessive Failed Logins" likely means that it can highlight both unauthorized use of accounts and attempts at brute-force attacks. While this set of data scored the highest, the percentage of detected anomalies was not as high, suggesting a discrepancy between the two. Data Exfiltration ranked lowest (479.61) and was recognized with almost 100% anomaly detection rate. Low-volume, high-impact anomalies are the type that the AI system performs the best on. This means that in the future, models could use both historical approaches to assess risks and active monitoring for any signs of unusual activity to ensure both common and critical threats are not missed [40]. Since the gap is significant, also look at how to adjust thresholds to ensure that incidents such as many failed login attempts are detected. It proves that using both ways of measuring data helps to detect malicious acts in cloud databases with high accuracy.

5.2 Correlating the Strength of Predictions with Kinds of Vulnerabilities

Figure 6 expands the topic by reviewing the total prediction confidence for different types of vulnerabilities. The model ranked SQL Injection above all others indicating it is able to detect attacks based on their repeated patterns. This approach matches traditional research, where injecting SQL queries into a program is easier to notice because of its unusual coding and the use of added SQL keywords. Having high confidence in XSS and Privilege Escalation implies that the AI system can handle established code-injection threats. Predicting threats such as DDoS and Phishing became less certain [41]. This is likely because the attacks are caused by certain circumstances and how individuals behave. Such attacks are especially effective due to human mistakes and frequently leave no standard pattern in the network or system logs. Likewise, DDoS attacks may make internet traffic seem normal and harder to detect as an anomaly. Based on these results, the model is not able to process all types of threats evenly and therefore, showing the analysts how certain the prediction is could help them decide on the ideal response. Since the confidence of AI is inconsistent, it is reasonable to believe that cybersecurity AI should not function alone but with the input of human analysts [42]. If feedback loops and more relevant threat data were used, there would be less difference between low security threats and those with an extreme impact.

5.3 AI is used in detecting insider threat behaviors.

The research focuses on finding out how AI assists in detecting people acting as insider threats within cloud networks. Insider threats are dangerous because they can sneak past the outer protections and act normally, but with some unusual inclinations. This study's AI model is capable of finding the identified anomalies, mainly through noticing "Unusual Login," "Excessive Failed Logins," and "Malware Activity." This is what happens when someone in a leading role misuses their authority or loses their trust in the company. When using machine learning with supervision, the model analyses past malicious activity and has a chance to spot rising threats [43]. The ability to do this is essential in cloud databases, as continuous integration, providing access to users and allowing remote login

can provide risks. An unusual action like logging in from a new IP address at an odd time would be considered suspicious for any logged-in person, making security systems less dependent on simply reviewing 'rules.' Monitoring dynamic and large systems with AI is more effective than traditional log monitoring. Yet, there are drawbacks to using AI such as incorrect outcomes and issues related to keeping information private [44]. Consequently, using AI should go together with access control rules, educating users and real-time analysis of their actions for the strongest protection.

5.4 Drawbacks of Advanced IoT Detection Framework

Regardless of the significant performance seen in the results, there are several aspects of the current AI anomaly detection system that should be improved. Looking at Figure 5, the detection system could still miss threats, since some vulnerabilities have low anomaly scores. If there are too many similar alerts, they can cause people to become unconcerned. However, when there are few but very significant events, details that matter may be neglected because people focus more on them. The unbalanced situation may result in ineffective use of available resources [45]. The data we use is often limited in quality and the process of labeling it can be problematic too. For an AI model to do its best, it needs data that is properly labeled and comprehensive. In many practical cases, there is often a lack of accurate data about insider threats which affects the quality of training data. Furthermore, the old model can be vulnerable to unknown threats or modern methods of attack that are not like those seen before. Understanding how the results are obtained is not always clear. In industries such as finance and healthcare, where regulations are important, security analysts usually want to know why the AI reached a particular classification [46]. Unless AI systems are made interpretable, many people may not be able to trust them enough to use them. Fundamentally, adopting AI in anomaly detection improves enterprise cybersecurity, but long-term benefits can only be achieved by always checking the solutions, using hybrids whenever needed and openly considering all aspects.

5.5 Using context-aware knowledge to improve detection

AI-based cybersecurity systems will benefit from using context-aware learning models. With these types of machine learning, each incident is seen individually and other factors like who the user is and what their past activity shows are ignored. Context-aware systems would check user behavior looking at IP, timestamp, user role, last actions, current location and how others are behaving. A high number of login attempts can happen while people reset their passwords, yet it could also suggest a brute-force attack unrelated to password resets. This applies to data taken from a company outside paying customers' peak periods which can have varying risks according to the user and involved department [47]. With the help of such AI, there is a higher chance that both false alarms and missed issues will be fewer. Both Natural Language Processing (NLP) and Graph Neural Networks (GNN) can be useful tools for future research in log analysis. With these techniques, patterns that are not noticeable to regular models can be discovered. Therefore, to improve cybersecurity, we need AI models that can understand different situations.

5.6 Impacts of Cloud Security Operations on Enterprise Strategy

Cloud-using companies can utilize the learnings from this study for their strategic planning. Because digital transformation is speeding up, enterprise data is now largely managed by cloud databases and this has prompted an increase in threats from employees. AI-based anomaly detection systems provide a quick and efficient way to manage the challenges outlined above. Adopting AI at SOCs helps set up automated first-line security, so that professionals can spend their time analyzing major threats and dealing with them. Since AI can be less certain about some threats, it is important for companies to use dynamic systems that consider both the risks and the likelihood of AI errors. the research

highlights the role of ongoing learning in the teaching process [48]. Dynamic cloud environments often make it necessary to replace static models. Ensuring detection models are always updated can be achieved by implementing feedback loops in organizations. As a result, the system is both more secure and follows set guidelines like NIST, ISO/IEC 27001 and GDPR. As per the study, it is important for cybersecurity teams, data scientists and top management to collaborate. For AI in cloud security to work well, the culture in the organization must develop to ensure honesty, ethical thinking, and target business goals.

7. Future Works

This study has shown that AI can help detect insider threats in the cloud. Yet, due to constant changes in cybersecurity dangers and the cloud, continuous upgrades and improvements are needed. To enhance how accurate, effective, and useful these systems are, future investigations should focus on different essential aspects. When anomaly detection frameworks use XAI and consider the context, it will lead to a big improvement. Most of these black boxes are capable but provide no insight into why they gave that prediction. Whenever high stakes, as in healthcare, finance, or government activities, it is essential to make a machine learning system explainable so people trust it, it meets the law and guidance is given following an incident [49]. More research is needed to add features that generate visual explanations of both threats and the steps taken in decision-making. It would be beneficial to build real-time adaptive learning systems. Sometimes, supervised learning methods lose the ability to react to recent attacks due to their usual retraining process. Online and reinforcement learning would ensure that detection systems keep pace with advances, adapt to changes in the environment and learn what to expect from different threats, without anyone needing to make manual adjustments. Using logs from several sources such as biometric ID, customer sentiments and network behaviors, can help to identify compared to using one alone [50]. Combining this information with the help of advanced means such as GNNs or federated learning, will improve identification without impacting user data privacy. Ensuring privacy in AI through new types of models should be prioritized. Insider threat detection usually requires checking over sensitive data related to employees or the system. It is important for further research to examine how data can be protected with the help of differential privacy, homomorphic encryption, or secure multi-party computation. standard evaluation methods and systems are required to check the effectiveness of AI detection systems on different cloud networks. As a result, tests can be repeated, stakeholders will rely on trusting results and these technologies can be deployed faster. So far, the research has provided a basic level of understanding of AI-enhanced anomaly detection for cloud databases, but it should now investigate explainability, adaptability, data integration, privacy issues and standardization to make the most of AI for protecting cloud systems against insider threats.

8. Conclusion

It has been established in this research that artificial intelligence helps spot suspicious activities by insiders in cloud databases and therefore, effective anomaly detection must be included in cybersecurity systems nowadays. Because of the rise in cloud services and the growing sophistication of people threatening a business, basic rule-based systems cannot handle all the issues. This study reveals that using machine learning, behavior analysis and current sensor data with AI solutions allows for accurate, efficient, and instant detecting of unusual activities. Conducting analyses of failed logins, infection by malware, strange login times and data eviction from vital systems gave us an understanding of the trends leading up to insider attacks. Observing the prediction scores used for SQL injection, phishing and privilege escalation proved that AI models remain powerful under a variety of threats. Examining data and charts allowed this research to demonstrate how AI can

help discover inconspicuous patterns in big data sets. While the performance of AI models has improved, the research also mentioned that more focus is needed on explainability, adjustability and reliable ethics. Incorporating aspects such as context, adaptation and protection for personal data is necessary to deal with sophisticated threats from people inside an organization. Using AI for anomaly detection can greatly improve the security of cloud databases. Ongoing research and practical analysis allow a company to both improve its security and build a strong, open, and secure environment online. It offers a stepping stone to future progress in how AI can prevent breaches of sensitive information stored in the cloud.

9. References:

1. Nwachukwu, C., Durodola-Tunde, K., & Akwiwu-Uzoma, C. (2024). AI-driven anomaly detection in cloud computing environments.
2. Tarafdar, R. (2022). AI-Powered Cybersecurity Threat Detection in Cloud Environments. International Journal of Cybersecurity and Digital Forensics.
3. Stutz, D., de Assis, J. T., Laghari, A. A., Khan, A. A., Andreopoulos, N., Terziev, A., ... & Grata, E. G. (2024). Enhancing security in cloud computing using artificial intelligence (AI). Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection, 179-220. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394196470.ch11
4. Kasula, V. K., Yadulla, A. R., Konda, B., & Yenugula, M. (2024). Fortifying cloud environments against data breaches: A novel AI-driven security framework. World J. Adv. Res. Rev, 24, 1613-1626. https://www.researchgate.net/profile/Vinay-Kumar-Kasula/publication/387128793_Fortifying_cloud_environments_against_data_breaches_A_novel_AI-driven_security_framework/links/67d88b75e62c604a0ddcb6d3/Fortifying-cloud-environments-against-data-breaches-A-novel-AI-driven-security-framework.pdf
5. John, R., James, S., John, J., & Robert, W. (2022). Integrating AI-Based Anomaly Detection in Cloud Database Security Frameworks.
6. Gadde, H. (2023). AI-Driven Anomaly Detection in NoSQL Databases for Enhanced Security. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14(1), 497-522. https://www.researchgate.net/profile/Amelia-Ethan/publication/385720663_AI-Driven_Anomaly_Detection_in_NoSQL_Databases_for_Enhanced_Security/links/6732c19a69c07a411444cc7d/AI-Driven-Anomaly-Detection-in-NoSQL-Databases-for-Enhanced-Security.pdf
7. Emma, O., & Maxwell, D. (2024). AI Based Anomaly Detection Systems for Cloud Security: A Framework for Implementation. https://www.researchgate.net/profile/Emma-Oye/publication/390430874_AI_Based_Anomaly_Detection_Systems_for_Cloud_Security_A_Framework_for_Implementation/links/67ed7d449b1c6c487770e80a/AI-Based-Anomaly-Detection-Systems-for-Cloud-Security-A-Framework-for-Implementation.pdf
8. Samudrala, V. K. (2020). AI-powered anomaly detection for cross-cloud secure data sharing in multi-cloud healthcare networks. Current Science & Humanities, 8(2). https://www.jcsonline.in/admin/uploads/AI-POWERED%20ANOMALY%20DETECTION%20FOR%20CROSS-CLOUD%20SECURE%20DATA%20SHARING%20IN%20MULTI-

CLOUD%20HEALTHCARE%20NETWORKS.pdf

9. Gladwin, O. (2020). Next-Generation AI and Database Security: Innovations for Enhanced Cyber Threat Prevention. https://www.researchgate.net/profile/Oscar-Gladwin/publication/385410687_Next-Generation_AI_and_Database_Security_Innovations_for_Enhanced_Cyber_Threat_Prevention/links/67235149db208342dee098d1/Next-Generation-AI-and-Database-Security-Innovations-for-Enhanced-Cyber-Threat-Prevention.pdf
10. Hassan, Z. (2024). AI-Driven Mitigation Strategies for Insider Threats in Corporate Networks. Eastern European Journal for Multidisciplinary Research, 1(1), 30-45.
11. Muzaffar, J., & Mazher, N. (2024). AI-Powered Behavioral Analysis for Insider Threat Detection in Enterprise Networks. Baltic Journal of Multidisciplinary Research, 1(2), 1-11. http://balticpapers.com/index.php/bjmr/article/view/8
12. Saleh, S. M., Sayem, I. M., Madhavji, N., & Steinbacher, J. (2024, November). Advancing Software Security and Reliability in Cloud Platforms through AI-based Anomaly Detection. In Proceedings of the 2024 on Cloud Computing Security Workshop (pp. 43-52). https://dl.acm.org/doi/abs/10.1145/3689938.3694779
13. Yasani, R. R., Prasad, P. M., Srinivas, P., Reddy, N. R. S., Jawarkar, P., & Raghunath, V. (2024, November). AI-Driven Solutions for Cloud Security Implementing Intelligent Threat Detection and Mitigation Strategies. In 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC) (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/10837032
14. Banerjee, S., & Parisa, S. K. (2023). AI-Enhanced Intrusion Detection Systems for Retail Cloud Networks: A Comparative Analysis. Transactions on Recent Developments in Artificial Intelligence and Machine Learning, 15(15). https://www.researchgate.net/profile/Somnath-Banerjee-13/publication/390098593_AI-Enhanced_Intrusion_Detection_Systems_for_Retail_Cloud_Networks_A_Comparative_Analysis/links/67df828972f7f37c3e878ff3/AI-Enhanced-Intrusion-Detection-Systems-for-Retail-Cloud-Networks-A-Comparative-Analysis.pdf
15. Akbar, R., & Zafer, A. (2024). Next-Gen Information Security: AI-Driven Solutions for Real-Time Cyber Threat Detection in Cloud and Network Environments. https://www.researchgate.net/profile/Ali-Zafer-3/publication/385417618_Next-Gen_Information_Security_AI-Driven_Solutions_for_Real-Time_Cyber_Threat_Detection_in_Cloud_and_Network_Environments/links/6723b68277f274616d541f34/Next-Gen-Information-Security-AI-Driven-Solutions-for-Real-Time-Cyber-Threat-Detection-in-Cloud-and-Network-Environments.pdf
16. Aslam, S., & Jackson, M. (2022). AI-Driven Anomaly Detection: Strengthening Data Protection in Enterprise Networks.
17. Bin Mofidul, R., Alam, M. M., Rahman, M. H., & Jang, Y. M. (2022). Real-time energy data acquisition, anomaly detection, and monitoring system: Implementation of a secured, robust, and integrated global IIoT infrastructure with edge and cloud AI. Sensors, 22(22), 8980. https://www.mdpi.com/1424-8220/22/22/8980
18. Tariq, B., & Patel, H. (2021). Cloud Security Reinforcement: AI-Based DSPM and Machine Learning Anomaly Detection. https://www.researchgate.net/profile/Harry-Patel-7/publication/388578408_Cloud_Security_Reinforcement_AI-Based_DSPM_and_Machine_Learning_Anomaly_Detection/links/679ddd9e8311ce680c48421b/Cloud-Security-Reinforcement-AI-Based-DSPM-and-Machine-Learning-Anomaly-Detection.pdf

19. Steven, D., & Smith, J. (2024). Cloud-Native AI for Real-Time Anomaly Detection in Edge Computing.
20. Parker, O. (2020). AI and Cybersecurity in Modern Databases: Innovative Approaches to Threat Detection and Response. https://www.researchgate.net/profile/Oakley-Parker/publication/385410677_AI_and_Cybersecurity_in_Modern_Databases_Innovative_Approaches_to_Threat_Detection_and_Response/links/67234f9b77f274616d53e5aa/AI-and-Cybersecurity-in-Modern-Databases-Innovative-Approaches-to-Threat-Detection-and-Response.pdf
21. Ajala, O. A., & Balogun, O. A. (2024). Leveraging AI/ML for anomaly detection, threat prediction, and automated response. World Journal of Advanced Research and Reviews, 21(1), 2584-2598. https://wjarr.co.in/wjarr-2024-0287
22. Ji, I. H., Lee, J. H., Kang, M. J., Park, W. J., Jeon, S. H., & Seo, J. T. (2024). Artificial intelligence-based anomaly detection technology over encrypted traffic: A systematic literature review. Sensors, 24(3), 898. https://www.mdpi.com/1424-8220/24/3/898
23. Hudson, J. (2024). Artificial Intelligence and Cybersecurity Integration: Modern Database Techniques for Securing AI Models. https://www.researchgate.net/profile/Jack-Hudson-6/publication/385410990_Artificial_Intelligence_and_Cybersecurity_Integration_Modern_Database_Techniques_for_Securing_AI_Models/links/67235fba77f274616d53f71c/Artificial-Intelligence-and-Cybersecurity-Integration-Modern-Database-Techniques-for-Securing-AI-Models.pdf
24. Inaganti, A. C., Ravichandran, N., Nersu, S. R. K., & Muppalaneni, R. (2021). Cloud Security Posture Management (CSPM) with AI: Automating Compliance and Threat Detection. Artificial Intelligence and Machine Learning Review, 2(4), 8-18. https://scipublication.com/index.php/AIMLR/article/view/129
25. Anayat, R. (2024). AI in Cloud Security: Strengthening Data Protection in Multi-Tenant Environments. https://www.researchgate.net/profile/Rakshanda-Anayat/publication/388526086_AI_in_Cloud_Security_Strengthening_Data_Protection_in_Multi-Tenant_Environments/links/679bd7508311ce680c4476eb/AI-in-Cloud-Security-Strengthening-Data-Protection-in-Multi-Tenant-Environments.pdf
26. Mamidi, S. R. (2024). Dynamic Security Policies for Cloud Infrastructures: An AI-Based Framework. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 1(1), 200-211. https://newjaigs.com/index.php/JAIGS/article/view/159
27. Sourag, V. T., & Sagayam, M. S. (2024). Investigating How AI and Machine Learning can be Leveraged to Enhance Cloud Security by Predicting and Preventing Cyber Threats. Frightening Future of Business Researches in Public Policy and Social Science Domains, 119. https://www.ijrbs.com/wp-content/uploads/2024/12/7.%20Sourag%20V.T%20&%20Maria%20Sabastin%20Sagayam.pdf
28. Rehan, H. (2021). Leveraging AI and cloud computing for Real-Time fraud detection in financial systems. Journal of Science & Technology, 2(5), 127. https://www.researchgate.net/profile/Hassan-Rehan/publication/390466223_Leveraging_AI_and_Cloud_Computing_for_Real-Time_Fraud_Detection_in_Financial_Systems/links/67eef01576d4923a1af30ca6/Leveraging-AI-and-Cloud-Computing-for-Real-Time-Fraud-Detection-in-Financial-Systems.pdf
29. Hudson, J. (2024). Revolutionizing Database Security with AI: Exploring the Latest

Advances in Cybersecurity.

30. Bibi, P. (2022). Artificial Intelligence and Database Security: Cutting-Edge Techniques for Cyber Threat Mitigation. https://www.researchgate.net/profile/Palwasha-Bibi-2/publication/385411024_Artificial_Intelligence_and_Database_Security_Cutting-Edge_Techniques_for_Cyber_Threat_Mitigation/links/672358a177b63d1220d00ca5/Artificial-Intelligence-and-Database-Security-Cutting-Edge-Techniques-for-Cyber-Threat-Mitigation.pdf
31. Ofili, B. T., Obasuyi, O. T., & Osaruwenese, E. (2024). Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats. Int J Eng Technol Res Manag, 8(11), 631.
32. Kenzie, F. (2021). Securing Databases with AI: The Latest Techniques in Cybersecurity for Intelligent Data Systems. https://www.researchgate.net/profile/Florence-Kenzie/publication/385410859_Securing_Databases_with_AI_The_Latest_Techniques_in_Cybersecurity_for_Intelligent_Data_Systems/links/672354772326b47637bce6bc/Securing-Databases-with-AI-The-Latest-Techniques-in-Cybersecurity-for-Intelligent-Data-Systems.pdf
33. Mamidi, S. R. (2024). The Role of AI and Machine Learning in Enhancing Cloud Security. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 3(1), 403-417. https://newjaigs.com/index.php/JAIGS/article/view/161
34. Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57(5), 132. https://link.springer.com/article/10.1007/s10462-024-10776-5
35. Olawale, O. P., & Ebadinezhad, S. (2024). Cybersecurity anomaly detection: Ai and ethereum blockchain for a secure and tamperproof ioht data management. IEEE Access. https://ieeexplore.ieee.org/abstract/document/10680041
36. Nzekwe, C. J., & Ozurumba, C. J. (2024). Integrated strategies for database protection: Leveraging anomaly detection and predictive modelling to prevent data breaches.
37. Johnson, S. (2024). Harnessing AI for Insider Threat Detection: Strategies for Proactive Mitigation in Corporate Networks. http://mzresearch.com/index.php/MZJAI/article/view/458
38. Joha, M. I., Rahman, M. M., Nazim, M. S., & Jang, Y. M. (2024). A Secure IIoT Environment That Integrates AI-Driven Real-Time Short-Term Active and Reactive Load Forecasting with Anomaly Detection: A Real-World Application. Sensors, 24(23), 7440. https://www.mdpi.com/1424-8220/24/23/7440
39. Joseph, A. (2024). AI-driven cloud security: Proactive defense against evolving cyber threats. International Journal of Computer and Information Engineering, 18(5), 261-265. https://www.researchgate.net/profile/Ashley-Jose-4/publication/380487517_AI-Driven_Cloud_Security_Proactive_Defense_Against_Evolving_Cyber_Threats/links/663e7bcc06ea3d0b7458a68d/AI-Driven-Cloud-Security-Proactive-Defense-Against-Evolving-Cyber-Threats.pdf
40. Kavitha, D., & Thejas, S. (2024). Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE Access. https://ieeexplore.ieee.org/abstract/document/10747338
41. Parker, O. (2020). AI-Driven Cybersecurity: The Role of Database Technologies in Strengthening Data Defense. https://www.researchgate.net/profile/Oscar-

Gladwin/publication/385410684_AI-Driven_Cybersecurity_The_Role_of_Database_Technologies_in_Strengthening_Data_Defense/links/672350d4db208342dee09716/AI-Driven-Cybersecurity-The-Role-of-Database-Technologies-in-Strengthening-Data-Defense.pdf

42. Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2024). Enhancing cloud security: The role of artificial intelligence and machine learning. In Improving security, privacy, and trust in cloud computing (pp. 85-112). IGI Global Scientific Publishing. https://www.igi-global.com/chapter/enhancing-cloud-security/338350
43. Oye, E., & Clark, A. (2021). AI-Enhanced Network Security Monitoring in AWS: A Practical Approach. https://www.researchgate.net/profile/Emma-Oye/publication/390266608_AI-Enhanced_Network_Security_Monitoring_in_AWS_A_Practical_Approach/links/67e673f08a5ab03f9717adf8/AI-Enhanced-Network-Security-Monitoring-in-AWS-A-Practical-Approach.pdf
44. Madhuvantha, K. A. N., Hussain, M. H., De Silva, H. T., Liyanage, U. I. D., Rupasinghe, L., & Liyanapathirana, C. (2021, December). Autonomous Cyber AI for Anomaly Detection. In 2021 3rd International Conference on Advancements in Computing (ICAC) (pp. 85-90). IEEE. https://ieeexplore.ieee.org/abstract/document/9671203
45. Pentyala, D. K. (2024). Artificial Intelligence for Fault Detection in Cloud-Optimized Data Engineering Systems. International Journal of Social Trends, 2(4), 8-44. https://www.yuktabpublisher.com/index.php/IJST/article/view/186
46. Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. Internet of Things, 23, 100887. https://www.sciencedirect.com/science/article/pii/S254266052300210X
47. Khan, A. Y., Latif, R., Latif, S., Tahir, S., Batool, G., & Saba, T. (2019). Malicious insider attack detection in IoTs using data analytics. IEEE Access, 8, 11743-11753. https://ieeexplore.ieee.org/abstract/document/8930920
48. Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing. https://era.library.ualberta.ca/items/72d03629-a6ac-4e5d-8528-3f10b552cda7
49. Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial Intelligence-Based Cyber Security and Digital Forensics: A Review. Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 391-419. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394303601.ch18
50. Parveen, N., & Basit, F. (2023). Securing Data in Motion and at Rest: AI and Machine Learning Applications in Cloud and Network Security.
51. Dixit, P., Bhattacharya, P., Tanwar, S., & Gupta, R. (2022). Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey. Expert Systems, 39(5), e12754. https://onlinelibrary.wiley.com/doi/abs/10.1111/exsy.12754
52. DatasetLink

    https://www.kaggle.com/datasets/rasikaekanayakadevlk/integrated-security-and-user-incident-management