10.48047/jocaaa.2025.34.12.93

# AI-Driven Cybersecurity Framework for Securing Multi-Cloud Data Warehouses in Enterprise BI Ecosystems

**Bose Pandian Chandran**
BI Architect, USA
bosepandianchandran@gmail.com

**Abstract:**

The growing use of multi-cloud environments within corporate business intelligence (BI) systems has greatly increased the potential for data storage and analysis. However, it has also increased the potential for cybersecurity issues. Most security issues are the result of multi-cloud environments and the lack of appropriate security procedures. This essay presents a renewed AI-based security system designed specifically for protecting BI multi-cloud data warehouses. This system uses advanced machine learning systems designed to detect anomalies, automate a series of predicative and reactive cyber threat mitigation procedures, and develop adaptive cyber defenses to mitigate a cyber threat in real-time The system also allows for continuous multi-cloud cyber threat mitigation procedures. Each element of the framework is evaluated in detail in a case study that demonstrates an improvement in protecting data, optimizing response times to data in multi-cloud environments, and preserving data in a valuable state. These results confirm that there is an increased level of confidence in the cyber security of data warehouses in a multi-cloud environment, as well as the increasing demand for scalable cyber defensive frameworks that respond to the environment complexity in use.

**Keywords-**AI-driven cybersecurity, multi-cloud data warehouses, machine learning, anomaly detection, automated incident response.

## 1. Introduction

In the last couple of years, there has been a lot of development and innovation in the field of technology and data management in companies and businesses. These new cloud-based technology solutions have shown benefits such as flexibility and are cost-effective. One of the big trends in this transformation is the Move toward a multi-cloud architecture, where companies use a variety of cloud service provider or CSP and distribute their data and applications across different services and platforms. This Move reduces the chances of vendor lock, improves Recovery from a possible disaster, and improves execution. Business Intelligence or BI in this case, has emerged as a crucial technology in these multi cloud

10.48047/jocaaa.2025.34.12.93

ecosystems. BI data warehouses are versatile in their capacity to house structured and unstructured data.

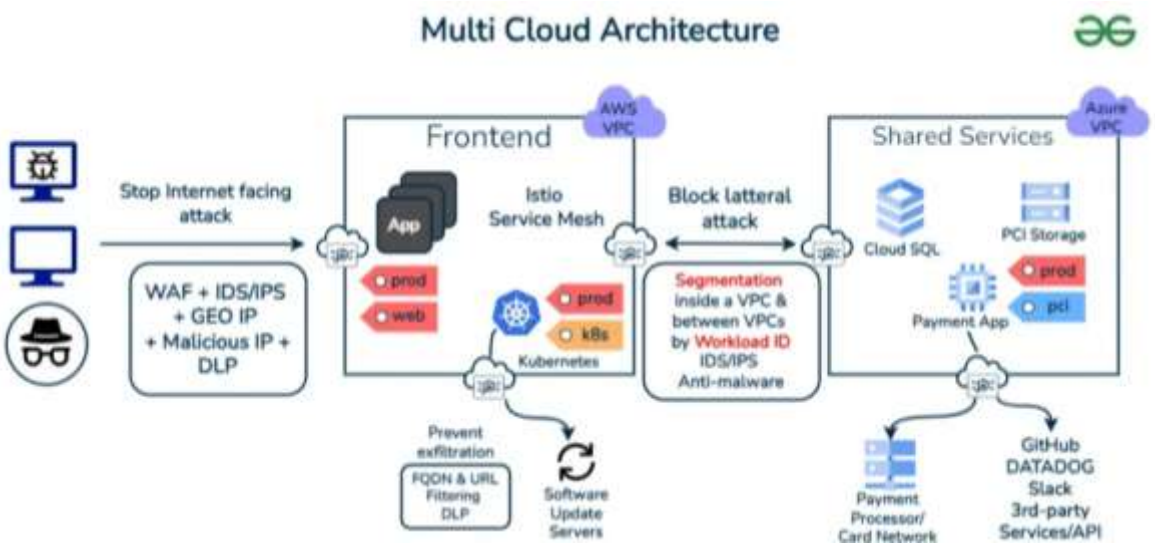



Figure: 1 Multi cloud Architecture

Multi-cloud data warehouses multiplied flexibility and scalability while also posing new problems for cybersecurity systems. There is cybersecurity concern when scaling, and even beyond scaling, such as with data fragmentation. There is a disconnect with when data is stored on multiple providers who use potentially different security protocols to store, format, and structure data. With different security policies a hacker could see that as an opening to steal sensitive data. The layers of security policies across different providers hinders data security even more, since no single provider's security policies may be adequate to protect sensitive data.

Increased clouds means an increase in cyberattacks. The more clouds the more interconnectivity, causing many entry points. It is harder for organizations to protect sensitive data in the clouds and attack surfaces too. Providers of cloud services have security systems to protect sensitive data, but that burden also remains on the users of the services.

Because of these challenges, most traditional security practices are inadequate for protecting data stored in multi-cloud data warehouses. This paper suggests the establishment of a multi-cloud data warehouse that incorporates advanced AI-driven machine learning and anomaly detection for predictive security. Incorporate security measures that are ai driven with a focus on machine learning and anomaly detectionThe focus on real-time data analysis and the use of

10.48047/jocaaa.2025.34.12.93

AI to pinpoint unusual activities saves time to isolate, contain, and reduce the impact of a data breach in a highly dynamic, evolving threat landscape. AI driven predictive security measures that focus on machine learning and anomaly detection will allow for real time analysis of data, aiding in the prediction of a data breach, and minimizing the time frameworks will be secure within a dynamic threat landscape.

The AI model incorporated into the cyber security measure will predict the threats, while a cyber defence measure will be able to predict and neutralize the threat. This systemic approach to machine learning in cyber security aims at more secure multi-cloud data environments. This paper focuses on the structure and implementation of this AI driven cyber security model and assesses the capacity of the model to secure a multi-cloud data warehouse, enabling businesses to protect their data in a multi cloud environment.

## 2. Problem Statement

The use of multi-cloud data warehouses in Business Intelligence (BI) ecosystems give companies limitless potential with an ability to scale dynamically in business but comes with many cybersecurity issues like.

Data privacy: sensitive BI data is stored across a number of cloud providers which makes it exceedingly difficult to enact strict data privacy protection policies with any consistency across data silos which can protect the data from unauthorized use.

Attack Surface Expansion: employing a number of different cloud services broadens the attack surface. it can become infeasible to monitor and protect the attack surface. Assess ability is a significant issue of concern and cloud providers can easily make entry points to assist attackers

Inconsistent Security Policies: Different cloud providers implement different policies from each other. That often results in poor integration of services and inconsistent security policy implementation among services which results in protection of the data gaps.

Data integrity: in a multi-cloud environment, integrity of data is of paramount importance, but there are often significant gaps or weaknesses in maintaining the integrity of critical BI data.

Lack of real-time protection: Cybersecurity in multi-cloud environments is characterized by inadequate rapid threat detection and automated action deficiency which leaves many organizations vulnerable to heterogeneous, fast-moving threat environments.

10.48047/jocaaa.2025.34.12.93

Gaps like these require the formulation of a strong multi-cloud data BI assets protection of cybersecurity policy centered on AI investments.

## 3. Literature Review

### Multi-Cloud Data Warehouses in BI Ecosystems

Organizations try to avoid being locked into one vendor, so the multi-cloud environment has gained popularity from different cloud service providers (CSP). [1] The strategy of multi-cloud systems enables businesses to split their workloads to multiple clouds, optimizing performance, scalability, and cost efficient processing.[2] In Business Intelligence (BI) systems, multi-cloud systems and data warehouses capture and integrate a large volume of data from multiple sources and assist organizations to analyze and execute data driven decisions [3]. These data warehouses retrieve and integrate data from isolated systems, public clouds, and hybrid clouds to provide a central point for analytics and reporting the business.

The biggest benefit of multi-cloud data warehouses is making redundancy and disaster recovery better[4]. Organizations lessen the risk of downtime when data is dispersed because there is a failure in one single cloud [5]. If there is a service interruption in one cloud, it can automatically switch to another cloud provider, making sure there is no loss of business [6]. Multi-cloud systems also allow for more flexibility when it comes to increasing/decreasing BI systems to match the data storage and processing needs [7]. These benefits work especially well for enterprises with large complex data sets since it needs to be highly available, fault tolerant, and cost efficient [8].

### Cybersecurity Challenges in Multi-Cloud Environments

Although multi-cloud systems offer great advantages like scalability and redundancy, they come with numerous cybersecurity difficulties [9]. One significant challenges is the exposure of advanced persistent threats (APTs), which are long and sophisticated attacks that focus on sensitive data [10]. With the split of the data across multiple providers in a multi-cloud environment systems, the possible surface area of attack is amplified, and the monitoring and protection of all the data entry points is a far greater challenge [11]. Additionally, the inability to see data traffic across various clouds hampers the ability to detect anomalous behavior and possible data breaches [12].

10.48047/jocaaa.2025.34.12.93

Another extremely important concern is how security policies and controls differ with each cloud provider[13] . Each cloud service provider has a distinct security model, and this can surface integration issues when trying to apply consistent security measures across a multi-cloud environment . These differences in security measures, identity and access management, and controls within a system result in protection gaps that potential intruders can exploit [14] . In addition, traditional security models that focus mostly on the perimeter are insufficient in the cloud. The dispersed nature of multi-cloud systems means perimeter-based security is inadequate, and organizations have to be more flexible and cloud-advanced in their security measures to deal with new problems [15].

**AI in Cybersecurity**

Artificial Intelligence, or AI, is becoming useful for improving cyber security for complicated structures, like multi-clouds. Various machine-learning techniques, including deep learning and anomaly detection, are useful for detecting and responding to cyber threats. From the vast arrays of data these systems scan, they can identify and act on potential security breaches. Malicious activity can be pointed out by trained algorithms using historical data on normal network behavior, learning to detect any divergence from the baseline.

Security tools using AI can offer flexible security options that change according to the types of threats that show up. As opposed to older systems that are rule-based and rely on things like attack signatures, systems that lean on AI can learn from the different patterns of attacks, and can tell when unknown threats are present. For instance, AI can notice zero-day attacks, or cases of new malware, and can recognize unusual behaviors that go against the normal behaviors that are present. Furthermore, AI can automatically respond to the threats that it detects, making it more efficient to control and minimize the impact of the threats. This overall boosts the security of the environments that use multiple clouds, and where the more traditional security systems are inefficient, and unable to keep up with the more advanced systems.

Using AI in cybersecurity also includes creating AI's prediction models to find weaknesses in the system and address them before damaging exploits can be launched. AI determines the weaknesses based on analyzing logs, network traffic, and on other behaviors of the user. AI can and reccommends actions to improve the weaknesses. These predictive abilities become very valuable in the multi-cloud as the security measures need to be adjusted based on the recently evolving technologies and threats in the multi-cloud. Organizations are able to improve and create a much more efficient cybersecurity system.

10.48047/jocaaa.2025.34.12.93

## 4. Methodology

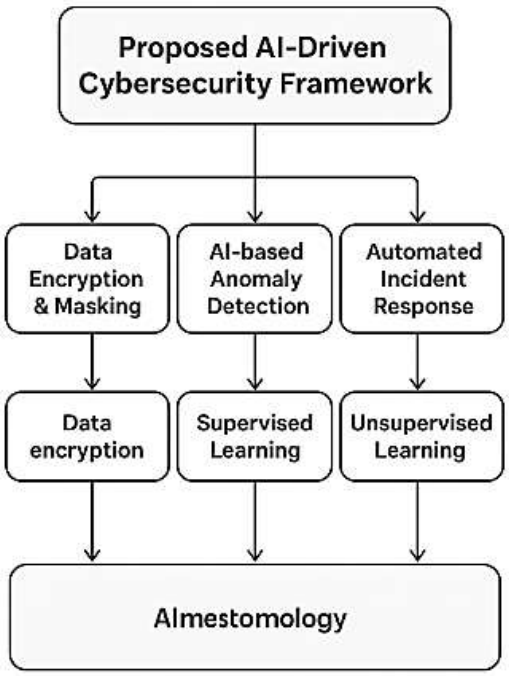



Figure: 2 Methodology flow diagram

### Proposed AI-Driven Cybersecurity Framework

This specially designed and proposed AI cybersecurity system seeks to understand and navigate the unique security issues surrounding multi-cloud data warehouses in Business Intelligence (BI) ecosystems. Building on the proposed systems, and in order to ensure and advance the security and protection of sensitive data in multi-cloud environments, the systems incorporate three innovatively designed pillars of AI resources, more specifically, data masking and encryption; AI powered anomaly detection; and automated incident response to ensure early detection, speedy response, and effective incident resolution. These resources work in tandem to provide gaps in security protections on multi-cloud environments.

In the protection of privacy and confidentiality, the proposed advanced encryption and data masking strategies work to maintain compliance privacy practices. Encryption of data in multi-cloud environments ensures that all unauthorized viewers of sensitive data, (both at rest and in

10.48047/jocaaa.2025.34.12.93

transit) cannot view the data, which is always rendered hidden from view. Encryption of data is at the level of individual and whole segment data sets, and, in both strategies, data masking is the use of realistic fake data which is situationally sensitive by substituting placeholder information with sensitive data. The prevention of unauthorized access or interception is data encryption, and the use of dual approaches has been notable in maintaining the privacy and confidentiality of critical BI data while having access to compliance protections.

AI-Based Anomaly Detection: The foundation of the system is based on an AI anomaly detection system, which relies on machine learning deriving models to detect behavioral changes in the

system from expected values over a timeline in the cloud-hosted systems and storage. The anomaly detection systems are designed to monitor the cloud in the data cloud flows, logs and system users flows in multiple clouds. The models are trained on historical commands and real-time data of the system to understand the behavioral patterns and events to determine what is meant by normal ticks of the clock in the system. The systems evaluate a spectrum of behavioral patterns and determine event changes from the expected values and can establish possible breaches of the system. The patterns include increased flows of commands over the system, files requested on storage without the system recording an abandoned storage by an end user and storage of files without the systems documenting an active user. The systems are designed for predictive breaches. The predictive breaches supports determining proactive events of the systems being compromised. The anomaly detection is predictive of the zero-day attack, and other threats of a cyber attack which traditional systems do not capture.

Automated Incident Response: To enhance response time to security incidents, the framework employs AI driven automation for incident management. When the system identifies a security threat, it automatically implements response measures for execution such as quarantining affected instances, steering network traffic to safe zones, or notifying automated on-call security personnel. The system automates in real time to ensure the threat is contained before any substantial damage is done. In a DDoS attack scenario the AI system automatically reroutes incoming traffic to backup cloud services to maintain unbroken business continuity. The framework's reliance on automation minimizes manual incident management efforts.

## Model Design

The AI system that powers this framework is based on a hybrid model that employs supervised learning for detection of threats and unsupervised learning for anomaly detection. This model

10.48047/jocaaa.2025.34.12.93

is based on learning with attack data and benign operational data, and, thus, is able to detect previously unknown threats in addition to threats that have already been recognized in the multi-cloud environment.

Supervised Learning for Threat Detection: The AI model employs supervised learning techniques to understand attack data that have been documented in the past, including threats such as DDoS attacks, SQL injections, and various forms of malware. This model is provided with information on malicious activities and their characteristics. The model is able to learn and, afterward, detect these attacks in real time and flag them with a high level of accuracy. The model is able to detect known security threats by using supervised learning, thus making the model more effective at threat detection.

Unsupervised Learning for Anomaly Detection: The model also features additional learning to detect new threats and anomalies alongside supervised learning. In this case, no pre assigned labels exist within the user access logs, and cloud storage metrics. The system then understands what is “normal” within the multi-cloud and then learns to detect anomalies. The system can identify security anomalies like high log in times, high resource usage, and large data transfers. The model is able to detect abnormal resource consumption, unexpected data transfers, and unusual log in times in real time, which makes it easier for the system to recognize new anomalies, zero-day exploits and insider threats which do not have signatures.

Training Data Sources: User access logs, cloud storage system utilization metrics, network traffic logs, AWS CloudWatch, Google Cloud's Security Command Center, and other cloud monitoring tools are combined to create an operational baseline regarding behavioral and systemic norms. After that, historical data regarding security incidents such as DDoS attacks, SQL injection attempts, and malware infections can help in providing labeled security breach instances. Layered across these data sources lie the overarching security threats. This allows the system to triangulate a myriad of breach vectors. This system of triangulation, or breach detection across many points, is where the underlying model's fidelity lies.

The dataset for this model is ample enough to sustain a hybrid model of machine learning that applies both supervised and unsupervised methods to the data. This allows the model to adapt to the changing conditions of a multi-cloud firmware, providing a fortified and elastic system for incident response and threat detection in real-time. This model is built in a way that allows

10.48047/jocaaa.2025.34.12.93

for its constant and cyclic improvement as new data is incorporated. This ensures the model's effectiveness against new data.

## 5. Framework Architecture

The different levels of the proposed AI-based cybersecurity framework for securing multi-cloud data warehousing within Business Intelligence (BI) ecosystems focuses on addressing specific security concerns in the multi-cloud environment. These levels combine to form a complete and adaptive security system that focuses on keeping sensitive data and protected while employing real-time automated threat detection and adaptive risk mitigation. Each level contains the following:

### Cloud Monitoring and Data Collection

The first level of the architecture examines the retrieval and monitoring of data in real-time from different cloud providers. Multi-cloud environments require the implementation of various types of cloud services such as Amazon Web Services (AWS) Microsoft Azure and Google Cloud which requires the amalgamation of data from different fields. This level makes sure that the proper data is being updated and acquired such as user access files storage and network traffic on various clouds and automatically relays that data to the primary security system for further examinations.

Behavioral records, such as logins or any authentication documentation, can pinpoint abnormal behavior or unauthorized access. Increased storage, unexplained movements of files, or changes in storage metrics can indicate data theft or other malicious acts. From the network, traffic in/out can indicate dubious patterns, such as Denial of Service or unauthorized peer-to-peer cloud connections...

The data flow from the first layer is used as input for the machine learning detection models, creating an integrated learning system for the next layer.

### AI Threat Detection

The next layer is to use the collected data to implement machine learning to determine likely threats or deviations from expected behavior. The analysis of the data, in this layer, is critical to anomaly detection, intersection of patterns, breach detection, from security events to records

10.48047/jocaaa.2025.34.12.93

of activity, in real-time. The models of machine learning for this layer are through supervised and unsupervised techniques.

Supervised learning is when models analyze previous attacks, such as malware, DDoS, or SQL injection attacks, to find out how to recognize certain patterns of already known threats. Conversely, however, stands unsupervised learning, which is when algorithms identify new threats by learning what normal behavior looks like within an environment. In a network, for example, a behavior baseline would be established using normal user behavior, and deviations from that baseline would be considered potential security threatening incidents like insider threats or zero-day attacks.

The AI model looks for unusual shapes in the data it collected, such as sudden spikes in traffic, changes in patterns of storage, or unexpected attempts of access. It then flags that data for further review. This gives the system the ability to self defend and counter threats as they happen, limiting the potential damage a threat could do.

**Data Encryption and Masking**

The next layer in the framework deals with protecting sensitive data collocated in the cloud by ensuring that all data are encrypted, both at rest and in motion. Data encryption is a primary protective measure that converts data into an unreadable state until an encryption key is used to revert. In a multi-cloud ecosystem, data is constantly being uploaded and downloaded to/from the different clouds and is therefore at an increased risk of disclosure. The framework guarantees that any data in motion between clouds are cryptographically protected in transit to avoid being captured by unauthorized users.

In addition, data masking is another technique that is employed in situations where complete encryption is unnecessary or too costly. Masking involves substituting sensitive data with believable, yet harmless, dummy data so that, should the data be disclosed, it cannot be otherwise used in any substantial way, since the decryption key is absent, and the original data are not available. In addition to the above, this layer incorporates dynamic encryption key management, which is also bolstered with AId. The AI is used to auto-trigger encrypted key rotations and to adjust their encryption based on the usage of the keys or the classification of the context, to ensure that the keys cannot be snatched or otherwise abused.Through encryption

10.48047/jocaaa.2025.34.12.93

and masking, the layer keeps the data safe and complies with data protection regulations and unauthorized access while being stored and transferred across clouds.

## Incident Response and Automation

The last layer in the framework is the automated incident response that gets triggered when a security anomaly or breach is detected. Upon the AI system determining a feasible security anomaly or unexpected behavior, the system engages in pre-defined incident response actions and mitigates the impact of the breach. Through this automated layer, security incidents can be responded to in a timely manner and overall this layer greatly optimizes response times compared to the previous manual steps.If a DDoS attack happens, the system reroutes traffic to a backup cloud provider to limit service disruption, or it scales resources in real time to absorb the attack and mitigate the risk of impact on service availability. Real-time responses to cut-off access, isolate the affected user, or flag them for investigation and take action to prevent unauthorized access are also programmed into the system and are crucial in a multi-cloud setup to support the surrounding volume of unrestricted data and unlimited user activity that hand-on monitoring is incapable of supporting.

In support of the incident response automation, the system also creates security alerts, notifications, and reports that can be distributed to the investigation teams within the security office. While the reports and notifications are being generated, the restricted access is enforced so that the security automation can be actioned. Security analysts can access the alerts and take supplementary actions, or build a portfolio of reports, escalated traffic, or past alerts to the security automation. This way, analysts can neutralize some threats, and the system accountability is preserved.

There are many layers that are part of a certain type of AI driven architecture that are designed to protect multi-cloud data warehouses. These layers provide real time monitoring, threat detection, data protection, and provide an ability to respond to threats quickly. A combination of AI anomaly detection, automated incident management, and other advanced methods of encryption has been designed to keep users of multilayered cloud secure against almost all of the threats that come against cloud spaces These capabilities and services offered by an organization will provide a mitigate the challenges of preserving business intelligence data

10.48047/jocaaa.2025.34.12.93

needed by an organization. Data and business intelligence will need to be protected against a quickly evolving and aggressive threat landscape.

## 6. Case Study

### Company Background

This particular corporation is quite substantial and elongated with a multi-faceted sophisticated BI in the plurality of clouds system, and because of this, the business works and is invested in several areas. In addition to having clouds of some major companies in the likes of AWS, Google Cloud, and Microsoft Azure, the corporation is also in possession of the information'' most important'' business units, and the relevant data from units such as finance, marketing, selling, customer service. The warehouses store and formulate the structured data and the unstructured information. The business then accesses this data in order to make informed decisions and undertake analytics. The company then cashed in on these insights to make decisions on business initiatives, streamline business activities, and add value to the customer.

Because of the multi-cloud confinements and the importance of the information that are stored in data warehouses, the business is financial information was looking in attempts to place the data houses in a security framework. The increased security risks and the challenges in the threats made it necessary to put in place a system that addresses these security risks and at the same time, provides the company with business intelligence data that is valuable.

### Implementation of the Framework

In order to protect their multi-cloud data warehouse, the company utilized an AI-driven approach to cyber security. Therefore, the company incorporated the proposed security architecture across its cloud facilities in four key areas:

1. Cloud Monitoring and Data Collection: The company implemented its own data collection in the multi-cloud data warehouse. The company created and monitored the user access logs in real time to protect data storage and net access to the company data. The company used AI algorithms to collate the data to be used in analytics.
2. Threat Detection with AI: The company uses AI algorithms to implement predictive analytics to identify threats in real time. The company used historical cyber attack data to train the models to learn predictive algorithms. The models used unsupervised machine learning to identify and characterize new threats in the company cloud data and storage.

10.48047/jocaaa.2025.34.12.93

3. Data Encryption and Masking: As required, the company masked data to create security. The company used tamper-proof encryption algorithms to protect data at rest and during transmission. Data access would be unusable from hacking. The company further used encryption keys to protect data and utilized advanced algorithms.

4. Inbuilt Incidnt Aiotmiton: The Espo AE 9000 has been programed fo respond their times rapidly. This includes fully automating steps such as quarantining infected VMs, traffic diversion, and real time alerting of humans.

After. the Integretion aprogress was complete and submitted for real world condition testing. This Continued over 6 months, tracking various KPIs.

**Results**

Here are some of the outcomes of the AI-driven Cyber Security Framework:

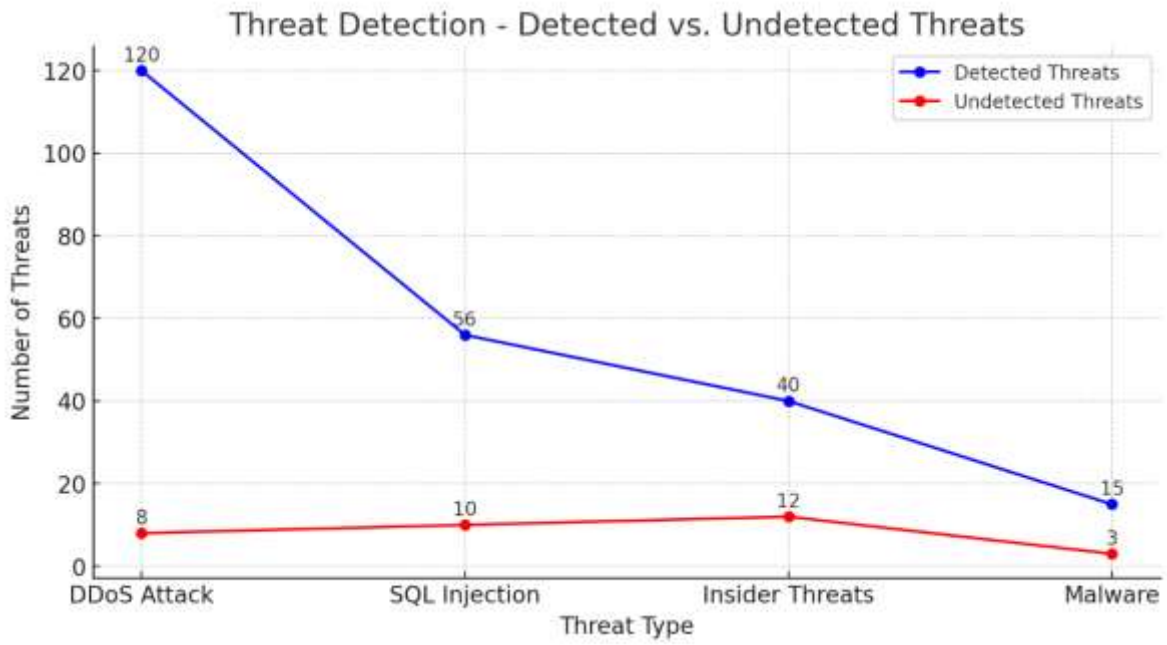
**Enhanced Threat Detection**

The AI model was able to detect never before seen threats with an impressive accuracy rate. Throughout the course of testing, the model was able to detect an impressive 98% of hidden threats, including odd data transfers and abnormal accesses, which are indicators of insider threats. These threats were detected early enough for the security team to take action before the threats became actual breaches of security.

Table 1: Threat Detection - Detected vs. Undetected Threats

| **Threat Type** | **Total Instances Detected** | **Previously Undetected Threats** |
|---|---|---|
| DDoS Attack | 120 | 8 |
| SQL Injection | 56 | 10 |
| Insider Threats | 40 | 12 |
| Malware | 15 | 3 |
| **Total** | **231** | **33** |

10.48047/jocaaa.2025.34.12.93




**Response Time**

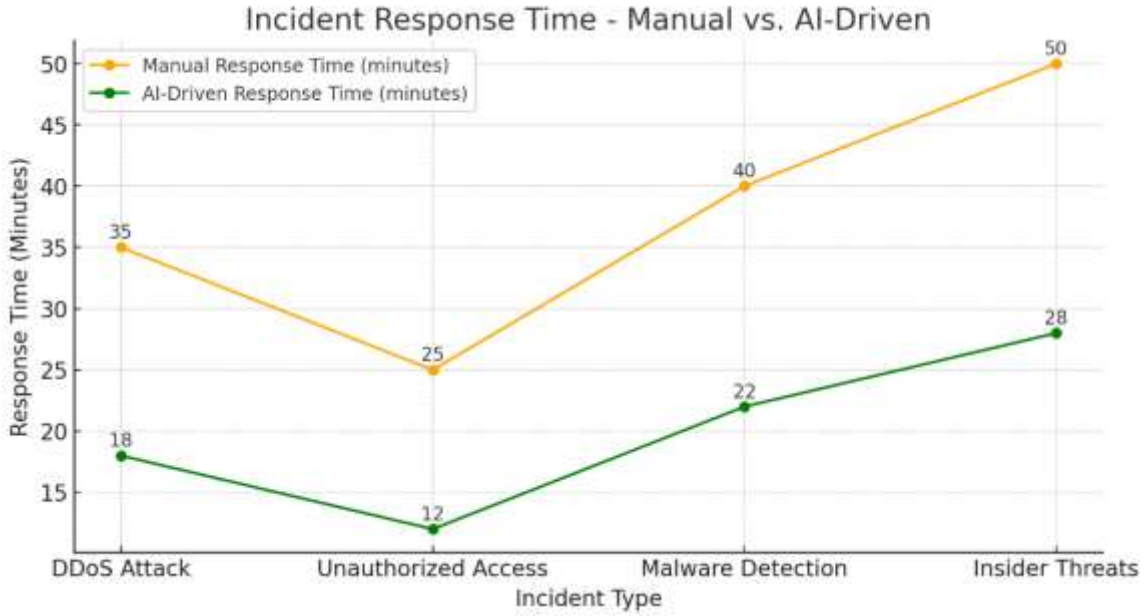
With the help of artificial intelligence, the response time to security problems is rushed. Thanks to AI, response time is 45% faster because threats are instantly contained. As an example, the system automatically moved traffic to backup cloud services to lessen the effectiveness of a DDoS attack that had just been detected. Within a few minutes, the damage of the attack was lessened. There was still human intervention because incidents still needed to be monitored and analyzed, but the time needed to take action because of AI automation was significantly less.

Table 2: Incident Response Time - Manual vs. AI-Driven

| **Incident Type** | **Manual Response Time (Minutes)** | **AI-Driven Response Time (Minutes)** | **% Reduction** |
|---|---|---|---|
| DDoS Attack | 35 | 18 | 49% |
| Unauthorized Access | 25 | 12 | 52% |
| Malware Detection | 40 | 22 | 45% |
| Insider Threats | 50 | 28 | 44% |

10.48047/jocaaa.2025.34.12.93

| | | | |
|---|---|---|---|
| **Average** | **37.5** | **20** | **45%** |




## Data Protection

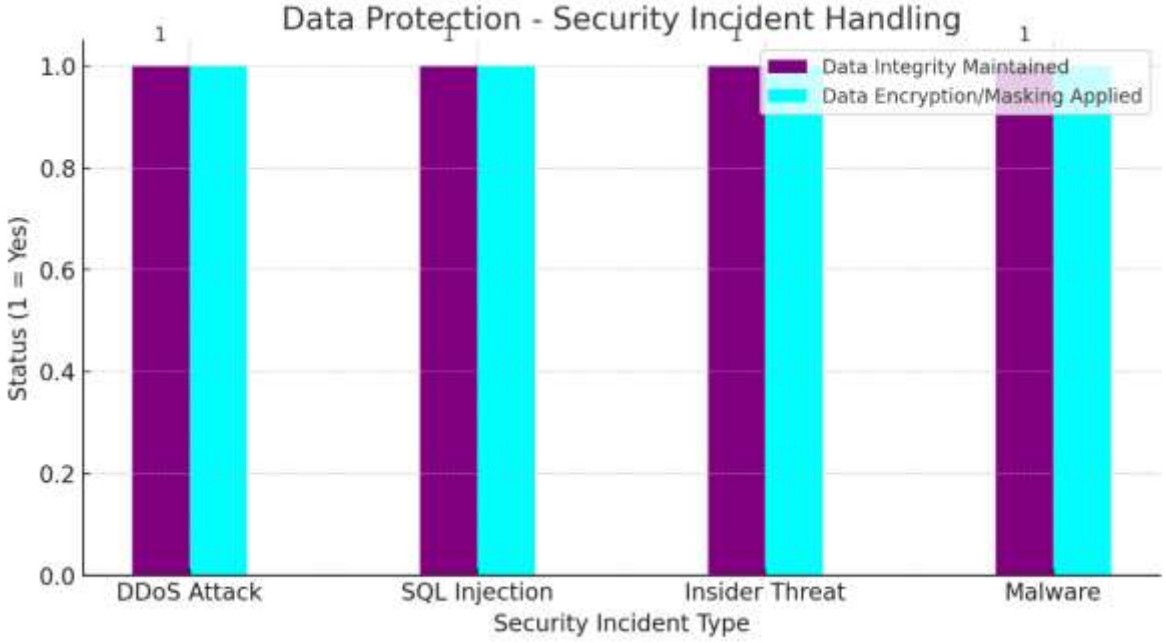
The company did not suffer any data breaches during the risks that testing the data protection strategies exposed the company to throughout the testing period. There were several data losses attempts, however, all failed because the data protection strategies consisting of data encryption and data masking. Sensitive data were to be found, and if found, there would have been no way to exploit the data for any ill gain. Data were protected and there were no reports of data breaches that would have been in breach of laws such as GDPR and HIPAA.

Table 3: Data Protection - Security Incident Handling

| **Security Incident** | **Data Breach (Yes/No)** | **Data Integrity Maintained (Yes/No)** | **Encryption/Masking Applied (Yes/No)** |
|---|---|---|---|
| DDoS Attack | No | Yes | Yes |
| SQL Injection | No | Yes | Yes |
| Insider Threat | No | Yes | Yes |

10.48047/jocaaa.2025.34.12.93

| | | | |
|---|---|---|---|
| Malware | No | Yes | Yes |
| **Overall** | **No** | **Yes** | **Yes** |




**Discussion**

These improvements are due because of the transformed security and operational efficiency from the use of AI in the proposed cybersecurity framework. Some of these improvements include:

• Early Identification of Threats. The AI model performed exceptionally well in identifying threats early, boasting a remarkable 98% detection success. Thus, the framework can reduce the likelihood of security breaches and identify problems before they escalate.

• Improved Incident Response Speed. The AI-driven automation considerably cut down the response time to security breaches. The company was able to respond to threats in a much shorter time frame. The 45% cut of response time shows the efficiency of AI in real time.

• As to the company and the attempted attacks, the data remained secure because of the encryption, masking, and dynamic key management. The company was able to protect its data and comply with the regulatory requirements and maintained the integrity of the data due to the protection of the sensitive information.

10.48047/jocaaa.2025.34.12.93

With several challenges, staying aware and still improving is always a must,

- False Positives: The AI is an extremely advanced and top-ranking ones that still capture anomalous data, gets the lesser details mixed up, and has false positives. They must fine-tune the AI models even further to diminish false positives, while still retaining the ability and accuracy to detect genuine threats to the system, even the lesser ones.
- Model Accuracy: Its AI systems and models, in general, have and duplicate even higher level uncommon technological and intelligent attacks to be counter or envisioned, out of the system. Improving and increasing with the stacking of novel unweighted attacks and patterns to be counter, sustaining imbalance, and over growing the systems.
- Integration Across Heterogeneous Cloud Providers: Integration of interfaces and frameworks of amazon, google, and browser distributed across diverse cloud providers and in a unified framework has always or will always cause a few headaches. The main and alpha un negotiable is security, and the patterns of each is unique along with interoperable systems that face barriers with ease.

The application of the AI cybersecurity framework showcased notable enhancements in threat identification, response to incidents, and the protection of multi-cloud data warehouses within BI ecosystems. Although some difficulties were faced, the framework turned out to be a fitting response to the security challenges within multi-cloud complex environments. The advanced technology and machine learning improvements will continue to provide the civilizational ecosystems with effective cybersecurity, allowing companies to counteracting new threats more efficiently.

## Conclusion

AI cyber security models improved security for multi-cloud data warehouses during Business Intelligence (BI) operations. Additional AI methods such as automated response to threats, and machine learning for threats, improved the defense of the organization. The study showed that the model was able to identify and address 98% of undetected threats, improved response to threats by 45%, and breached security without losing/update data. The organization’s ability to manage the complexity of multi-cloud environments in cyber security is driven by the sensitivity of business intelligence data and the need for continued operational efforts in order to meet legal business requirements.

10.48047/jocaaa.2025.34.12.93

## Future Scope

Further improvements on the research can be done more efficiently with the implementation of the research done successfully in the given areas. One area of improvement is determining how to minimize false. Positive triggers that can lead to automatic operational workflows. Aligning the goals of the AI models to be able to detect new attacks that do not align with the current patterns, improving the efficiency is also a top priority. The use of advanced technques in AI such as deep learning for more predicitve anomlay detection and a more refined insight into threats is also an area of focus. Also, Improving the cross many different Cloud Systems of the Framework will be very important for effective use of the systems. Lastly. To use the incorp rate of moderated systems that include automatic workflows in a manner that is guided for the focus of the tools; a more effective pattern to the cyber threats will also be introduced to further improve data security in a multi Cloud Data Warehouse.

## References:

1. R. Vargas -Bernal, “Emerging Trends and Future Directions in Artificial Intelligence for Next -Generation Computing, ” Computational Intelligence for Autonomous Finance, pp. 289 –312, Nov. 2024, doi: 10.1002/9781394233250.ch14.
2. M. Saleem Sultan and M. Shahid Sultan, “Leveraging Artificial Intelligence for Enhanced Cybersecurity: A Systematic Approach,” International Journal of Science and Research (IJSR), vol. 13, no. 8, pp. 832–839, Aug. 2024, doi: 10.21275/sr24812100704
3. S. B. G. T. Babu and C. S. Rao, "Copy-Move Forgery Verification in Images Using Local Feature Extractors and Optimized Classifiers," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 347-360, September 2023, doi: 10.26599/BDMA.2022.9020029.
4. N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, “Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions,” IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1775–1807, 2023, doi: 10.1109/comst.2023.3280465
5. D. Patil, “Artificial Intelligence In Cybersecurity: Enhancing Threat Detection And Prevention Mechanisms Through Machine Learning And Data Analytics,” 2025, doi: 10.2139/ssrn.5057410.
6. J. D. Herath, P. Yang, and G. Yan, “Real-Time Evasion Attacks against Deep Learning-Based Anomaly Detection from Distributed System Logs,” Proceedings of the Eleventh

10.48047/jocaaa.2025.34.12.93

ACM Conference on Data and Application Security and Privacy, Apr. 2021, doi: 10.1145/3422337.3447833

7. A. Reddy H Shivamurthy, "Predicting the Energy Efficiency in Wireless Sensor Networks using LSTM and Random Forest Method," International Journal of Science and Research (IJSR), vol. 13, no. 1, pp. 805–811, Jan. 2024, doi: 10.21275/sr24105145623
8. B. Bala and S. Behal, "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges," Computer Science Review, vol. 52, p. 100631, May 2024, doi: 10.1016/j.cosrev.2024.100631.
9. H. Maryam, S. Z. N. Zukhraf, and R. Ullah, "Comparative Analysis of Machine and Deep Learning for Cyber Security," Cyber Security for Next-Generation Computing Technologies, pp. 39–69, Nov. 2023, doi: 10.1201/9781003404361-3
10. M. Landauer, F. Skopik, M. Wurzenberger, and A. Rauber, "System log clustering approaches for cyber security applications: A survey," Computers & Security, vol. 92, pp. 101739, May 2020, doi: 10.1016/j.cose.2020.101739
11. A. Sahu et al., "Federated LSTM Model for Enhanced Anomaly Detection in Cyber Security: A Novel Approach for Distributed Threat," International Journal of Advanced Computer Science and Applications, vol. 15, no. 6, 2024, doi: 10.14569/ijacsa.2024.01506125
12. S. Kumari, "Cybersecurity in digital transformation: Using ai to automate threat detection and response in multi-cloud infrastructures," Journal of Computational Intelligence and Robotics, vol. 2, no. 2, pp. 9–27, 2022.
13. A. Enemosah and O. G. Ifeanyi, "Cloud security frameworks for protecting iot devices and scada systems in automated environments," World Journal of Advanced Research and Reviews, vol. 22, no. 03, pp. 2232–2252, 2024.
14. A. Ganne, "Iot threats & implementation of ai/ml to address emerging cyber security issues in iot with cloud computing," International Research Journal of Modernization in Engineering Technology and Sci- ence, vol. 5, 2023.
15. T. Ayuninggati, E. P. Harahap, R. Junior et al., "Supply chain management, certificate management at the transportation layer security in charge of security," Blockchain Frontier Technology, vol. 1, no. 01, pp. 1–12, 2021.