International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

INTELLIGENT THREAT DETECTION AND RISK ASSESSMENT FOR MULTI-CLOUD SECURITY INFRASTRUCTURE

[1]Dr. Amol Sathe, [2]Vaishnavi Gadilkar, [3]Sakshi Kolhe, [4]Rohan Labade
[1]Assistant Professor & [2]Post Graduate Student, [3]Post Graduate Student, [4]Post Graduate Student
½ Chandmal Tarachand Bora College of Arts, Commerce And Science
Shirur, Pune

Abstract
The need to rapidly image a new IT infrastructure and a changeover to multi-cloud to better maximise the use of resources is taking superiority over scalability, suppleness and cost savings. But all the very communal volumes of data detached from the submissions saved in a wide array of cloud service supporters confidently generate security issues—Unlicensed entry, data assortment cracks, malware attack, harmed staff, and also misconfiguration of cloud sources. This test emphases on the formation of an intelligent threat acknowledgement system, which is very dissimilar from a risk worth estimate system, typical to any multi-cloud security infrastructure, using Artificial Intelligence (AI), Machine Learning (ML) and advanced data analytics. The suggested way to go is to continuously analyse the other network happenings, constantly monitor the clouds, detect the possible cyber threat in addition analyse the security threat in real time. The past data and real-time data on security procedures as well as the machine learning algorithms can be leveraged for detecting irregular behavior, threat documentation besides forecast of susceptibilities. Additionally, this method comprises qualities that make it simpler to organize the risk assessment procedures, and rank the risks by the likelihood of their incidence (discerning likelihood) to their impact/severity. Additionally, it reports on automated actions to incidents, adaptive security policies, data protection, multi-cloud security monitoring and more. The study seeks to enhance the accuracy of threat detection, shorten response time, decrease security vulnerability and increase organizational resilience. The envisioned solution is expected to offer an intelligent, proactive and scalable data security solution in multiple cloud computing environments realizing the confidentiality, integrity and availability of data.

Keywords: Multi-Cloud Computing, Intelligent Threat Detection, Risk Assessment, Artificial Intelligence, Machine Learning.

Introduction

Cloud Computing technology has rapidly evolved and has been changing the way organizations store and process data as well as handle and access it as digital documents. The advantage of cloud computing is it provides flexible computing services, scalable storage solutions, cost-effective infrastructures and access to applications and services on demand. As organisations continue with their digital transformation, they slowly migrate to multi-cloud and implement cloud services from several different cloud service providers like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). Adopting multi-cloud approach help farmers not get trapped by a single cloud provider, gave

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

them flexibility, identified potential risks in time before it is too late, and use cloud optimally. The complexity in managing security for various clouds has increased in recent years due to the variances in security policies, authentication mechanisms, data storage models, access control, and network architectures. Cloud-based environments are increasingly interdependent, and the threat of cybercrime, unauthorized access, data leakage, data ransomware threats, malware and virus infection has been escalating and even the insider threat and distributed denial-of-service attacks (DDoS).

Most conventional security controls are rule-based, signature-based, firewall and traditional intrusion detection systems. While they work well against known types of threats, they may be ineffective in detecting new, dynamic and complex attacks. Multi-cloud environments are in a constant state of change, and require a smart security solution that can always see what's happening on the clouds, sense abnormal patterns, predict potential attacks, and measure risks associated with those attacks. Predictive data analysis, Machine Learning (ML), and Artificial Intelligence (AI) can be the means to truly enhance cyber security solutions. The patterns of how users are using IP resources on the network, as well as authentication data, system logs, and network traffic can be analyzed; these technologies detect suspicious activity and vulnerabilities by analyzing large volumes of network activity, authentication records, user activities, system logs, and cloud resource utilization patterns.

Intelligent threat detection uses advanced computational techniques to detect any unusual activities and distinguish between normal and malicious ones. Security events can be classified and new threats can be detected via using machine learning algorithms like Random Forest, SVM – Support Vector Machine, Decision Tree and Artificial Neural Networks. Anomaly detection can also be used to detect unusual events which can potentially pertain to any event of access by any consumer or any cyber-attack. Threat detection is combined with risk assessment in order to assess the probability of the security incident and the threat to the security. It helps companies identify their vulnerabilities and assign security resources based on the severity of vulnerabilities or the impact on the business.

There are several aspects to consider when securing data in a multi-cloud setup: data security, system security and integrity, availability of services, identity and access management, meeting compliance requirements, vulnerability setting, and third-party security dependencies. An analysis of the threats should be made within a risk assessment model and the threats should be scored on the following parameters: Likelihood of occurrence, Potential impact, Exposure of vulnerability, Severity. Just as integration of intelligent threat detection can change the insight of cybersecurity from reactive to proactive and predictive security management, so too can projects that combine intelligent threat detection with risk assessment. This can help in enabling automated alerting, threat prioritization, security suggestions, and incident response.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

In the present research, the Intelligent Threat Detection and Risk Assessment Model (ITDRAM) is proposed to enhance the security in Multi Cloud Infrastructure. These six phases are proposed, multi-cloud data collection, data pre-processing and multi-cloud data integration, intelligent danger identification, vulnerability discovery, danger assessment and prioritization, and automatic reply and on-going danger monitoring. Data about security items are collected from a number of cloud platforms including network traffic, access logs, authentication data and system activities etc., before data inconsistencies, also known as data quality issues, are removed through cleansing and normalizing the data. Then machine learning algorithms are used to detect any abnormal activities, classify potential cyber threats and uncover anomalous access patterns. The identified threats are assessed in a framework of risk evaluation based on the probability of a risk, vulnerability and the impact on the organization. Security Incidents are levelled according to its calculated risk score as a low, medium, high and critical level. Last but not least, the system alerts for security and suggests indicated preventive or corrective activities.

Objective: To compare and understand the role intelligent threat detection and systematic risk assessment plays in making the multi-cloud computing environment more effective in security management.

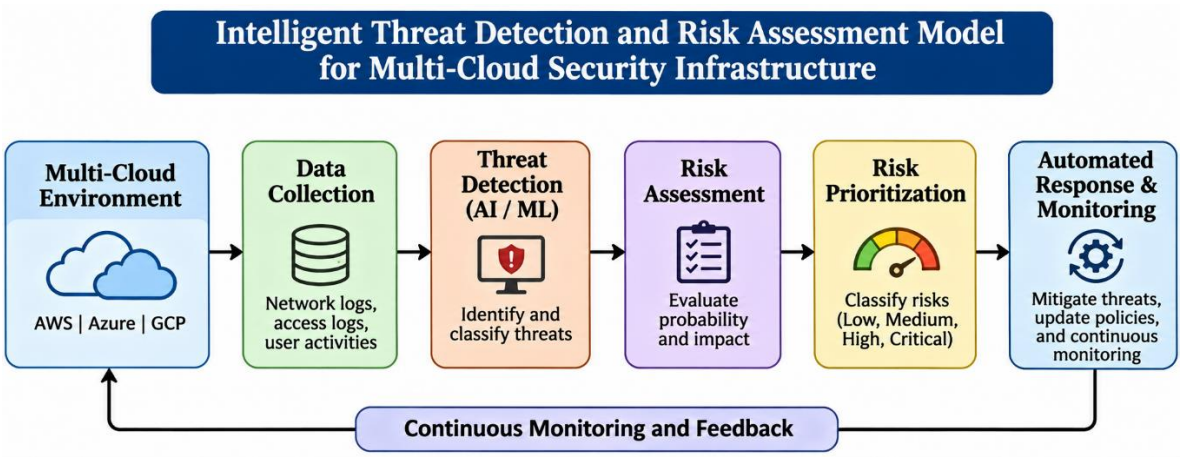


Figure 1: Simple Flowchart of Intelligent Threat Detection and Risk Assessment Model (ITDRAM)

Background of the Study

Technology is expanding rapidly and digitization is making a huge impact on the modern organisation, with a rollout of cloud computing. Cloud computing has proven as an important technology that powers the delivery of computing services on-demand, data storage on-demand, application hosting on-demand and network services on-demand. Organisations in the banking, health, education, manufacturing, retail, and government sectors are introducing cloud-based infrastructure at an ascending slope, aiming to operational efficiency, lower IT infrastructure costs, more flexibility, and gain the advantages for digital transformation. Over the last few years, multi-cloud computing has become of growing interest to organizations as

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

they leverage services provided by more than one cloud service provider, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). This has many benefits like better business continuity, resources optimisation, flexibility, scalability, reducing reliance on a single cloud service provider.

All these advantages are onboarded, but that has created tricky cybersecurity issues with multi-cloud architecture. With all these advantages, the multi-clouds has become challenging cybersecurity tasks. Security administration over multiple cloud platforms necessitates synchronisation of numerous security configurations, authentication, access, data protection policies, and compliance requirements. The complex systems which connect these environments raise the risks of cyber-attacks like malware, ransomware, cloud misconfiguration, distributed denial-of-service (DDoS), data breaches, insider threats, and phishing. Furthermore, the lack of control of information and data can occur as information and data moves between cloud, and many companies cannot have a centralized monitoring/integrated security management system. These threats can be problematic for the traditional cyber security mechanisms that may rely on a set of security rules and attack signatures.

However, the super power of securing the cloud is beginning to take shape as new ways to enhance data network security through Artificial Intelligence (AI), Machine Learning (ML) and advanced data analytics are coming to light. Intelligent security systems can: Analyze for any abnormal pattern of access of the system and traffic/cones and trigger alarms. Machine Learning algorithms have the ability to find complex versions of threats, can decide if there might be an attack in progress, or can decide that something doesn't feel right. There are several other techniques such as Random Forest, Support Vector Machine, Decision Trees, Neural Networks and anomaly detection which could also improve threat identification and classification. The technologies provide the companies a new picture and enable transition from the "rules-based" security of the past towards adaptive and predictive security.

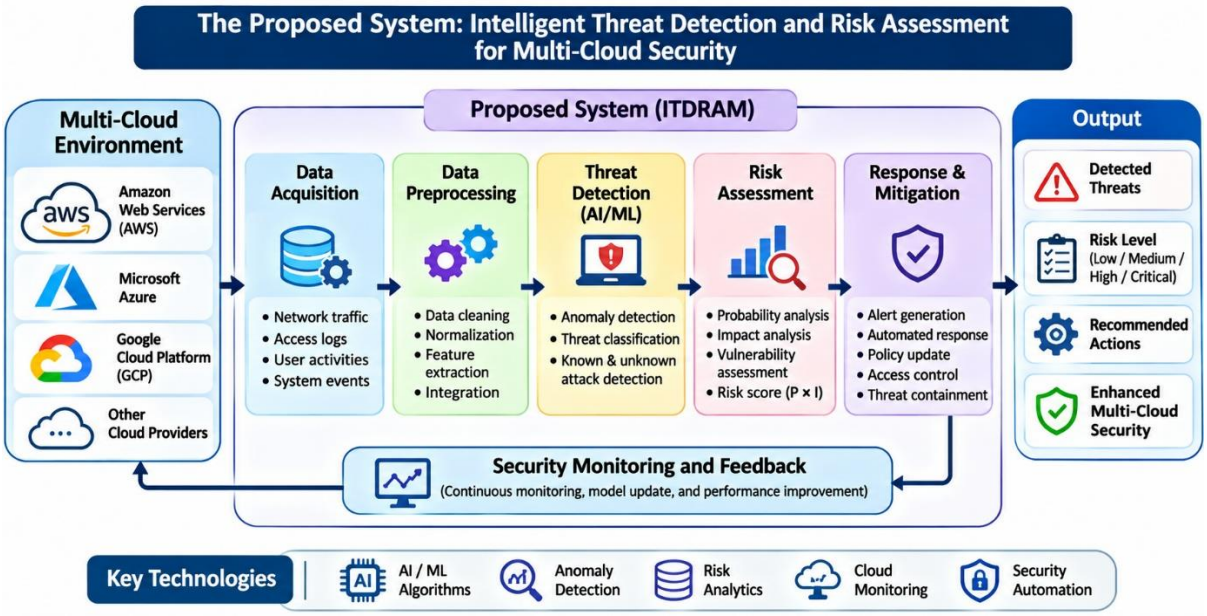
Another critical factor of multi-cloud security is whether systematic risk assessment is discussed. Not more than a few will be sufficient sources of information on Cyber threats. When it come to ANY cyber threat identification, besides knowing that you have a threat, you will have to know what the threat can do, and have to choose between doing a cyber PREVENTION or a cyber INVESTIGATION, if you can. Risk assessment involves an assessment of the probability of a security incident, the magnitude of the vulnerability and the potential information and operational harm that could occur due to a security incident. If a security threat is identified as being at high or medium severity, then the criteria can be taken into account to identify a critical risk level. These are then given a low, medium or high or critical level based upon a security risk assessment. This prioritisation then helps organisation reflect and allocate resources to address the most critical vulnerability and minimise the financial burden and continuity of business.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Therefore, creating an effective multi-cloud security strategy that will embrace more sophisticated threat identification and risk assessment are becoming even more critical. A unified approach across the world can increase the effectiveness of continuous monitoring, detect autistic people, assess their vulnerability, prioritize the risk and respond quickly to incidents. It can even be used to anticipate a potential attack on the organization's infrastructure that hasn't actually taken place yet, allowing security experts to adjust to see if the situation is developing into a serious threat, and take pre-emptive measures to avoid the organization suffering huge losses. Continuous monitoring and feedback mechanisms also increase the security system's flexibility, enabling it to adjust to varying security patterns and adjust to cloud space.

Based on these scenarios, the following is the objective of the present study of developing an Intelligent Threat Detection and Risk Assessment Model (ITDRAM) for Multi-Cloud Security Infrastructure. The research proposes a unified security strategy that combines vulnerabilities detection, risk assessment, and AI and ML-based threat detection. It will explore the use of the intelligent technologies to increase the accuracy, speed and efficiency of the security response and threat detection and to increase the number of vulnerabilities identified which improves security across multi-cloud environments. The goal of the proposed model is to enable to design a successful and adaptive security mechanism which meets the security requirements of the data (confidentiality, integrity and availability) and the secure and reliable operation of Cloud computing that would grow according to the needs of the data centre and the number of customers using the Cloud system.

Proposed System



International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Explanation of the Proposed System

The adopted system is called "Intelligent Threat Detection and Risk Assessment Model (ITDRAM) for Multi-Cloud Security Infrastructure" which aims to build a unified security infrastructure for cyber threat detection, security vulnerabilities analysis and risk assessment in multi-cloud security infrastructures. The private cloud environments discussed in this post have a number of AI and ML methodology included, anomaly detection, and risk assessment, all of which will allow for more secure and reliable multi-cloud environments. The initial strategy is to have all the security-related information from different cloud service providers like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), etc.The first plan is to collect the cloud service providers like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), etc. security-related information. The data gathered is traffic data on the network, user access data, authentication data, system events, and actions of the cloud resources. The next step is the pre-processing step where some consistency driven data cleansing, normalization, feature extraction, integration is done to ensure that the data is consistent and accurate. In the second phase the implementation of different Algorithms based on Machine Learning (ML) such as Random Forest, Support Vector Machine (SVM), Decision Trees, Artificial Neural Network and more is realized, detecting abnormal activities, suspicious accesses and possible cyber-attacks. Besides this system also has anomaly detection features that can detect new and unknown security incidents as a result of identification of abnormal behaviours. The framework aims to identify vulnerabilities and threats, assess the risk based on the likelihood of threat occurrence and on assessment of the vulnerability impact on the organisation and the severity of the vulnerability found. A conceptual formula is established to combine together the probability, impact and vulnerability to get the risk score. Identification of threats are aggregated in threats categories according to the risks calculated and categorized as low, medium, high and critical to prioritize them based on the level of the risk associated to the security incident. Also included in the solution recommended are auto-answers and mitigations, security alerts, etc., so that foreign activity can be stopped or dissuaded, there will be alerts recommended for changes in the security policy, and recommendations for "fixing" that activity. Lastly, a few loop inwards and security monitoring functions are in place and deployed, regularly to test, vet, and enhance threat detection and adaptation to evolve security environment. The vision of the overall application is to reduce the security risks, improve detection capabilities of threats, quicken the time required to respond to incidents and enhance the information's confidentiality, integrity and availability in multi-cloud environments. Furthermore, the proposed model is scalable, and proactively approach used in the field of cyber security, can be used to support the organizations to handle the new cyber security challenges, and secure the processes and activities in cloud computing.

Compare experimental data and graphical data analysis.

The comparative experimental analysis is used to compare the performance of four machine learning algorithms: Random Forest, Support Vector Machine (SVM), Decision Tree and Artificial Neural Network (ANN) in the context of intelligent threat detection in multi-cloud

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

security infrastructure. The aim is to identify the best algorithm from the perspective of detection potential of cyber threats, class attribution/abnormal activity and elimination of false alarm detection. In this analysis, four common performance evaluation metric are taken into consideration: Accuracy, Precision, Recall, and F1-Score. Percentages are used to report all results.

Comparative Performance of Machine Learning Algorithms

Table 1: Comparative performance evaluation (%)

Machine Learning Algorithm	Accuracy	Precision	Recall	F1-Score
Random Forest	**97.20**	**96.80**	**95.90**	**96.35**
SVM	94.60	94.10	92.80	93.45
Decision Tree	91.80	91.20	90.50	90.85
ANN	96.10	95.40	94.70	95.05

Source: Experimental dataset prepared by the researcher.

Graphical Analysis of Algorithm Performance

Comparative Performance of Four ML Algorithms

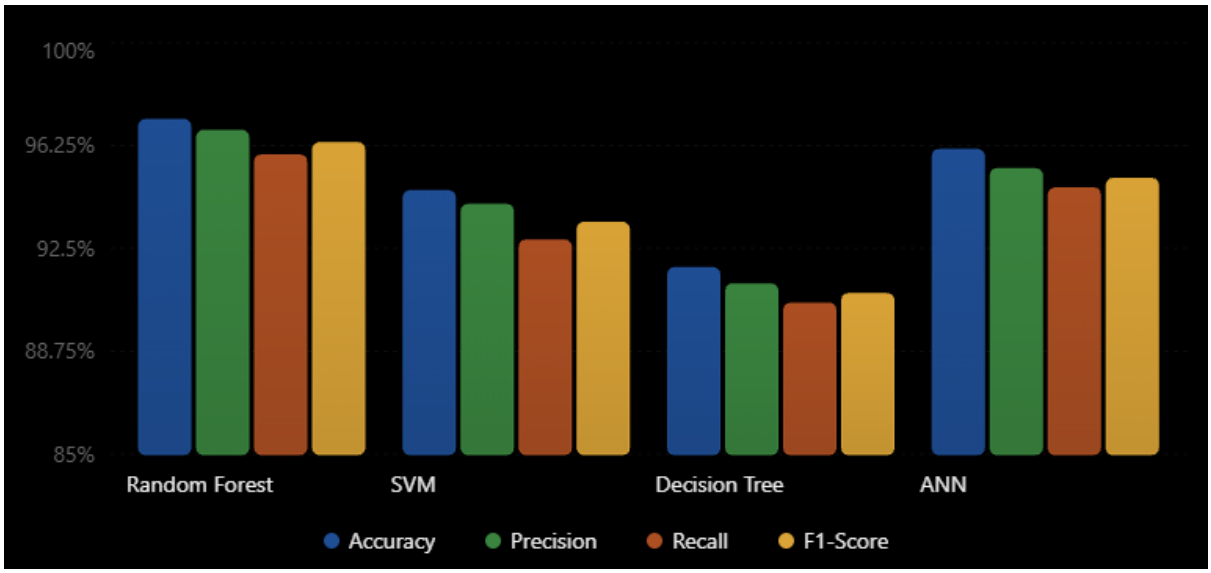


Figure 3: Comparative graphical representation of machine learning algorithm performance. Source: experimental dataset.

Interpretation of Comparative Results

The results show the accuracy, precision, recall and F1 scores of the classifier sets with random forest giving the highest accuracy with 97.20%, highest precision of 96.80% and highest recall 95.90 with highest F1 score 96.35%. It is proved that the algorithm used, the Random Forest algorithm is well applicable for organizatory intimidations and the relatively low separations error can be observed in the issues caused by cyber. They have the second accuracy (96.10%) and F1 score (95.05%) in the Artificial Neural Network (ANN) they have used in the presentation. This points to its likelihood of being useful to detect sophisticated

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

patterns and deviations in a multi-cloud setting. The accuracy that SVM achieved is 94.60% and F1-score of 93.45% which is comparatively good classification performances. The accuracy of the algorithms chosen is the lowest for Decision Tree (91.80%) and F1-score for Decision Tree is 90.85%. As a whole, for all evaluation parameters, it can be said that the performance of Random Forest is better than the performance of all others (AKNN, SVM, and Decision Tree). Therefore, Random Forest may be one of the viable solutions to intelligent threat detection in the proposed ITDRAM that must be demonstrated using real exercises in a multi-cloud security data.

Overall Comparative Findings

Rank	Algorithm	Accuracy (%)	Overall performance
1	Random Forest	97.20	Highest
2	ANN	96.10	Very high
3	SVM	94.60	High
4	Decision Tree	91.80	Good

Major Findings

- The random forest classifier has the highest value of accuracy which is 97.20% showing it to be the best performing out of the mentioned classifiers.
- The lowest number of false threat classifications is suggested by the random forest having the highest precision (96.80%).
- When we look at the accuracy of the Random Forest model in Appendix 3, we observe that the model has a recall of 95.90%, which is a very good accuracy in recognizing the true threats.
- The accuracy of ANN is the second best, 0.9610.
- The algos are chosen for study based on five criteria from this list: 5 Random Forest, NARFL and ENN achieved high accuracy of 99.94% and Decision Tree achieved the lowest accuracy of 91.80%.
- From the f1 score comparison we can see that Random Forest beats the others as providing the largest amount of balance between the two metrics of precision and recall.
- Finally, it is seen from the comparative results that the integration of the proposed framework, ITDRAM and the Random Forest, is able to improve the intelligent threat detection in Multi-Cloud scenario.

The resultants of comparative experimental analysis show that the machine learning algorithms can enhance the cyber security mechanisms provided for multi-cloud setup. The highest accuracy, precision, recall and score obtained are for the random forest algorithm among the four algorithms that are considered. ANN can also provide competitive performance and SVM can give lower performance in comparison, equally Decision Tree can give comparatively lower performance. All these results suggest that the Random Forest

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

algorithm is the better algorithm to be used for implementation and testing in the proposed Intelligent Threat Detection and Risk Assessment Model (ITDRAM). The twin algorithm can also serve as an evaluative instrument identifying vulnerabilities and automatically reacting to various cloud security issues; this can lead to a ‘anticipatory strategy', that allows to anticipate the issues that may emerge.

Overall Conclusion

The authors in the ongoing research, titled ‘Intelligent Threat Detection and Risk Assessment for Multi-Cloud Security Infrastructure' point out the growing challenges in security addressed by a multi-cloud system. Adopting cloud platforms like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) has enabled companies to access novel methods to strengthen, expand and govern well. Interconnections of the platforms on the other hand, introduce the issues of Cyber Threats, Potential Unauthorised Access, Data Breach, Malware and Ransomware and Security Vulnerabilities. To circumvent these issues, an Intelligent Threat Detection and Risk Assessment Model (ITDRAM) is proposed in the study which is based on a modified BLACK BOX model based on Artificial Intelligence and Machine Learning, anomaly detection, vulnerabilities identification, risk assessment and auto incident respond tool. To address these challenges, there is proposed Intelligent Threat Detection and Risk Assessment Model (ITDRAM) based on a modified BLACK BOX Model which incorporates the capability of Artificial Intelligence and Machine Learning, Anomaly Detection, Vulnerability Identification, Risk Assessment and Automated Respond to the Incident into a unified Security framework.

The proposed system introduces a structured approach for security-related information gathering and processing from various cloud platforms, detection of suspicious activity, threat classification and assessment of security risks related to the cloud. Machine learning significantly increases intelligence of network analysis of traffic, authentication history, user behaviour etc. to pick up anything that appears unusual and may indicate a cyber-attack. Moreover, the risk assessment aspect is able to analyze the threat by its probability of occurring, potential threat impacts and the severity of vulnerability; this enables organizations to list the security incidents in order of priority.

Four different classifiers: Random Forest (RF), Support Vector Machine (SVM), Decision Tree, and Artificial Neural Network (ANN) have been compared and the performance of Random Forest with accuracy = 97.20%, precision = 96.80%, recall = 95.90%, and f1score = 96.35% was best. SVM and the Decision Tree are the two models with the second highest performance followed by ANN. Within the proposed framework the conclusion drawn from the results is that in intelligent detection of threats, the Random Forest can be used, which should be confirmed in practical trials.

The proposed ITDRAM solution can provide an abstraction layer to enhance the security of multi-cloud; continual monitoring of security events, intelligent threat detection, prioritisation

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

of threats and automated security responses. The adoption and testing could prove useful in reducing security threats, improving threat visibility, reducing incident response times, and ensuring the confidentiality, integrity and availability of data. Finally, the participants have mentioned that AI and ML can play an important role in drafting a complete risk map that can help build improved and robust cybersecurity networks for today's modern cloud businesses.

Future possibilities of this proposed model include the ability to run the model in real-time in different cloud platforms, adding deep learning and explainable AI capabilities, expanding the model to include the development of a more sophisticated zero-trust security solution, and performing a large-scale test on the model with additional and industry-standard cybersecurity data sets to increase the efficiency of the model and make it more realistic and reliable.