International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I3P107

Volume 73 Issue 3, 57-63, March 2025

Original Article

AI-Powered Risk Assessment and Compliance in Cloud Cybersecurity

Thiyagarajan Mani Chettier[1], Venkata Ashok Kumar Boyina[2], Sandeep Rangineni[3]

[1]*Independent Researcher, South Windsor, CT, United States.*
[2]*Indepedent Researcher, Cumming, GA, United States.*
[3]*Independent Researcher, West Hills, CA, United States.*

[1]*Corresponding Author : thiyaga1980@gmail.com*

Received: 14 January 2025 Revised: 19 February 2025 Accepted: 11 March 2025 Published: 29 March 2025

Abstract *- Cloud Computing, revolutionary for digital infrastructure can potentially allow organizations to function at scale. While Cloud computing has its merits, it comes with new security threats and thus requires elaborate risk assessment and compliance processes. Utilizing ML and AI to improve threat detection, automate compliance monitoring, and reduce vulnerabilities, we present an AI-powered cloud cybersecurity risk assessment and regulation compliance approach. Apply behavioral analytics, anomaly detection, and predictive analytics to detect cyber threats before they happen. Artificial intelligence systems lower response latency to stop security breaches by monitoring data harvested from the cloud system for repeat behaviour patterns indicative of malefaction. The framework's real-time risk assessment allows organizations to prioritize security actions based on potential effects and probability. AI can sift through huge datasets to identify compliance gaps, recommend remedies, and deliver audit-ready reports while minimizing operational overhead and human error. Scalable architecture and the flexibility to respond to new cybersecurity risks make it an ideal system for use in multi-cloud and hybrid-cloud settings. It is a huge advantage for risk identification and compliance monitoring as this system has the potential to learn and adapt over time. This bolsters APT, zero-day, and insider threat defenses. Integrating AI with SIEM systems enhances incident response and real-time threat correlation. Some benefits organizations could enjoy by using AI for compliance management include reduced audit costs, improved security governance, and faster regulatory reporting. The finding indicates the necessity of AI applications to secure cloud environments and recommends further adoption within cybersecurity frameworks. Future studies will focus on improved AI-driven models toward cybersecurity, prioritizing explainability, ethical use of AI, and adapting regulations.*

Keywords *- Compliance Automation, Cloud Security, Risk Detection AI, Predictive Modelling, Anomaly Detection.*

1. Introduction

Most organizations moved to use processing besides the management of data. However, with the cloud being a new frontier, there are threats to cloud security that would be new to end users, including compliance issues, even though the cloud has multiple advantages like scalability, affordability, and operational flexibility.

Cyber-attacks are becoming advanced enough that existing security mechanisms are insufficient to protect cloud infrastructures. This is why AI-driven risk assessment and compliance solutions have become increasingly important in enhancing security and ensuring compliance. Finally, the unique deliverability, affordability, and flexibility offered by cloud computing have changed how businesses operate. As our cloud infrastructures expand, the old-school security mechanisms that were effective inside traditional IT environments were proven lacking in cloud environments.

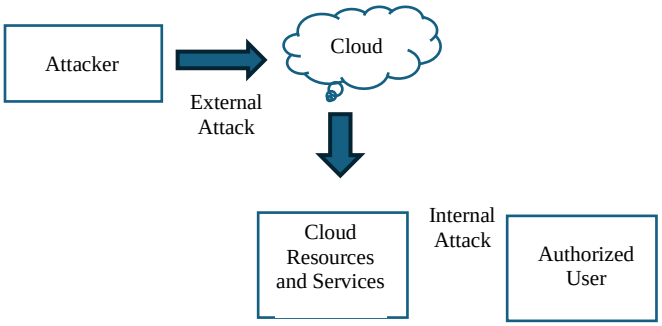


Fig. 1 Threat model for cloud computing

This transition results from AI making risk assessment and compliance frameworks significantly more dynamic and their ability to address cybersecurity challenges more proactively. In real-time, AI advancements enable the prevention of vulnerabilities by monitoring your cloud-based

environments to detect threats through advanced data analytics. Such smart technology can analyze large amounts of network data to look for patterns that could indicate cybercrime. This proactive capability reduces incident impacts of security breaches, improves precision in detecting threats, and decreases reaction times. Moreover, developing AI models will also enable continuous learning, which can be useful for risk assessment models that can be configured to adapt to the changing cloud environment and emerging cyber risks. These standards may be essential in terms of keeping the confidence of those who have an interest in the organization amassing and holding sensitive data safely.

Automated reviews, monitoring compliance with regulatory standards in near-real time, generating records of compliance gaps in real time, etc., are all AI-based compliance solutions. These levels of automation not only cut down on the administrative overhead of security staff and remove the chances for human error but also allow organisations to shift their focus on strategic risk management to quickly remediate a threat. Cloud Cybersecurity Framework: How Artificial Intelligence (AI) Can Transform Risk Assessment and Regulatory Compliance This discusses how AI helps automate some of the contentious areas in auditing and how to enhance compliance discussions by alleviating the burden of tracking the risk. AI-powered solutions enable organizations to build a cybersecurity architecture that is not only capable of preventing new attacks but is also agile enough to adapt to evolving regulatory mandates.

2. Review of Literature

The burgeoning interest in cloud computing has led to an increasing volume of literature on AI-enabled cloud cybersecurity risk assessment with a view to compliance. As organizations have turned to the cloud, advanced cyber-attacks have deepened in complex and ultimately very dynamic cloud environments, exposing rudimentary and pepperlike security techniques like audits and rule-based intrusion protection. Scientists have speculated on a means of employing a mixture of AI and ML methods to handle threat detection management, risk assessment administration and compliance monitoring over the cloud. Several studies highlight the critical need for AI-based risk assessment to enable real-time vulnerability detection and threat prevention.

Indeed, both supervised and unsupervised learning models in machine learning (ML) can parse through significant volumes of network traffic data to discover cycles and indications of a possible cyberattack (Gritti, C. et al., 2015). Likewise, He, D. et al. (2017) explain that deep learning algorithms are highly effective in reducing false positives in threat behaviour-based detection analysis compared with traditional regression models. The factors of predictive analytics have also been concentrated on in the literature as a key aspect of proactive cybersecurity. A possible methodology for an artificial intelligence (AI) risk assessment based on attack history is introduced by Wang C. et al. (2009) to forecast future security breaches. Their research shows how AI could inform decision-making to prioritize threats by likelihood and effect, and that's critical to help companies focus security resources where they'll do the best. As per their study, to adhere to regulations including ISO 27001, GDPR, HIPAA, and NIST, the program notes that AI-based solutions can continuously monitor security policies, identify rule violations, and suggest remediation.

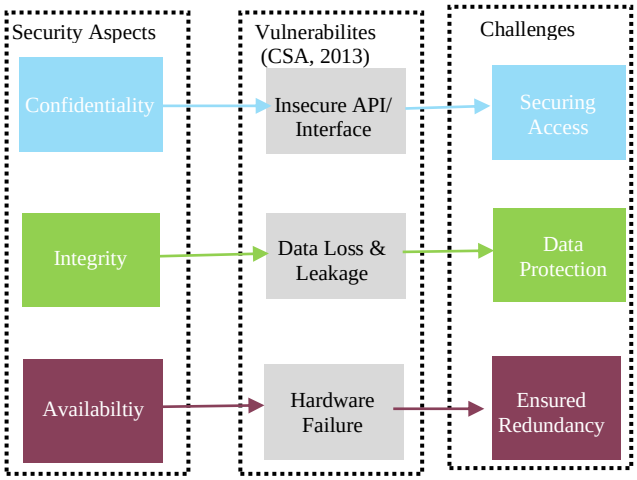


Fig. 2 Cloud Storage Security Aspects, Vulnerabilities & Challenges

Another work that interfaces with cloud security systems and uses AI to enhance compliance audits is Jansen, W. A.'s (2011) presentation. The research says automated compliance solutions simplify human auditors' lives by generating real-time reports and ensuring consistent compliance with cybersecurity regulations. AI for monitoring regulations could help organizations mitigate legal risks and fines. An integral area of AI-based cybersecurity frameworks is advanced threat detection. Jia, R. et al. (2021) The Role of AI in SIEM Systems. According to their findings, AI-augmented SIEM systems proved far more effective in identifying insider "threats, zero-day attacks, and distributed denial-of-service (DDoS)" strikes than their traditional counterparts. Also, Kene, S. G. et al. (2015) provide insights into ZTA and AI-powered Cybersecurity integration.

They discovered that AI could provide better user authentication, monitor privileged access, and assign security rules based on risk assessments. This adaptive security technique mitigates secure cloud infrastructure against internal attack and unauthorized access. Although it has many benefits, researchers have outlined some potential problems of AI-driven risk assessment and compliance. As Li, A. et al. (2019) and Ren, Y. et al. (2019) identify elements of non-explainability for AI models. Another major concern is data privacy (Shen, W. et al. 2017 and Wang, B. et al. 2012). AI must be vigilant around cloud-sensitive data, so it isn't leaking. To address this hindrance, researchers aim to develop more explainable AI (XAI) models, enhance the

cyber security governance powered by AI, and adapt AI to new cyber threats.

AI and blockchain integration specific to cloud security and compliance monitoring are still a work in progress. The literature review concluded that organizations benefited significantly from AI-driven risk evaluation and compliance automation , which enhances threat detection, risk prioritization, and compliance with regulations to bolster cloud cybersecurity.

Research indicates that AI-based protection through audits, predictive analytics, and machine learning can secure cloud infrastructures.

The openness of AI models, data privacy, and scalability remain chronic issues that warrant further investigation. As cyber threats constantly evolve, AI-based services will shape the direction of cloud security and compliance management.

2.1. Study of Objectives

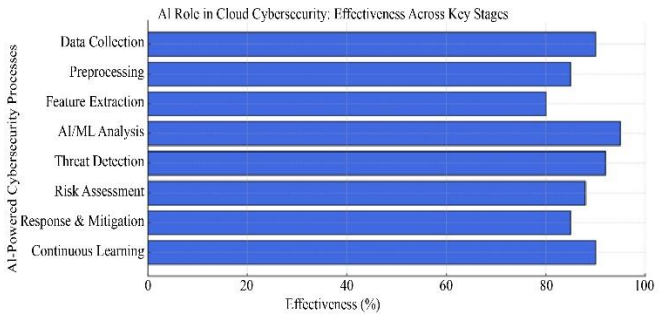
1. Investigating AI's Function in Cloud Cybersecurity.
2. To Establish a Framework for Risk Evaluation Driven by AI.
3. To enhance real-time threat identification and response.
4. To Assess the Capability and Flexibility of Artificial Intelligence in Concurrent and Mixed Cloud Sets.

3. Research and Methodology

The model output will show you what the problems or concerns could be. Compare the effectiveness of AI-driven risk assessments against more traditional cybersecurity approaches to detecting and combating attacks.

Develop strategies to integrate the AI models into existing cloud cybersecurity infrastructure. Feedback loops can be included to iteratively improve and adapt the model against new threats.

Examining artificial intelligence's function in cloud cybersecurity is made easier with this research method's organised approach. By collecting data and integrating models, this research hopes to show how artificial intelligence (AI) might improve cloud threat detection.




```
import numpy as np
import pandas as pd
from sklearn.ensemble import IsolationForest
from sklearn.metrics import classification_report

np.random.seed(42)

normal_data = np.random.normal(loc=0, scale=1,
size=(1000, 2))

anomalies = np.random.normal(loc=3, scale=1, size=(20, 2))

data = np.vstack([normal_data, anomalies])
labels = np.array([0]*1000 + [1]*20)

df = pd.DataFrame(data, columns=['feature1', 'feature2'])
df['label'] = labels

model = IsolationForest(contamination=0.05,
random_state=42)
df['anomaly_score'] = model.fit_predict(df[['feature1',
'feature2']])

df['predicted_label'] = df['anomaly_score'].map({-1: 1, 1: 0})

report = classification_report(df['label'], df['predicted_label'])
print("Classification Report:\n", report)
```

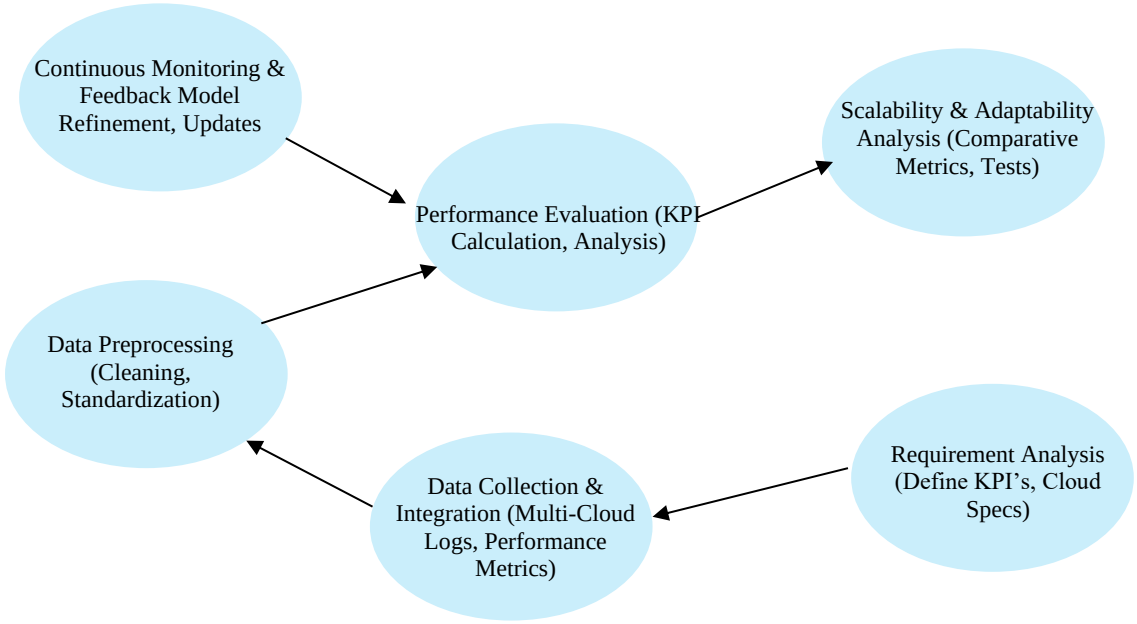
AI-Powered Anomaly Detection - Putting Concepts to Work Here, we will see how to implement AI-based anomaly detection by using the flow diagram below and the Python code sample, which will contribute towards achieving our objective of improved cloud security. By being a subject matter expert, you can detect such red flags as abnormal slow data transfers or an abnormally long time for logins. In evaluating AI, consider the three primary models of learning that exist: supervised, unsupervised, and semi-supervised.

We identify outliers and explore techniques for anomaly detection like Isolation Forests and Autoencoders. For example, the selected models can be trained by using historical data with known threat patterns. This section speaks about a systematic process of evaluating the impact of AI on cloud cybersecurity. The research suggests AI technologies may enhance cloud decision-making, vulnerability identification, and anomaly detection. The steps are as follows: Extraction of cloud activities logs, flow logs, and alerts, such as cloud security alarm logs, and established network traffic with a Cloud Service Provider (CSP). Different datasets (real-world and simulated) will guarantee a good coverage of both directions.

Preprocess the collected data: Fill missing information, remove duplicates, and standardize features. Feature selection allows data such as system logs, access patterns, and traffic volume to be enhanced with potentially impactful

insights. Look for statistical (and behavioral) indicators that may speak to dubious conduct. A Roadmap can be generated for building an AI-Powered Risk Assessment Framework for Cloud Cybersecurity using a systematic approach based on data-driven methodologies, model selection and continuous assessment. The methodology guiding the development process could be as follows:

Suppose AI systems need to grow and be flexible in multi-cloud and hybrid setups. In that case, a systematic process for collecting data, performance metrics, and the realization of actionable insights will help us properly evaluate the scalability and flexibility of the AI system. In this research, emphasis is given to the responsiveness, resource utilization, and workload adaptability of the AI systems distributed in different cloud infrastructures.




```
import weka.core.Instances;
import weka.core.converters.ConverterUtils.DataSource;
import weka.classifiers.bayes.NaiveBayes;
import weka.classifiers.Evaluation;

import java.util.Random;

public class RiskAssessmentFramework {
public static void main(String[] args) {
try {

DataSource source = new
DataSource("cloud_security_data.arff");
Instances dataset = source.getDataSet();

dataset.setClassIndex(dataset.numAttributes() - 1);

NaiveBayes naiveBayes = new NaiveBayes();

Evaluation evaluator = new Evaluation(dataset);
evaluator.crossValidateModel(naiveBayes, dataset, 10, new
Random(1));
System.out.println("=== AI-Powered Risk Assessment
===");
System.out.println("=== Cross Validation Results ===");
System.out.println(evaluator.toSummaryString("===
Summary ===", false));
System.out.println(evaluator.toClassDetailsString());
System.out.println(evaluator.toMatrixString("=== Confusion
Matrix ==="));

naiveBayes.buildClassifier(dataset);

        for (int i = 0; i < 5; i++) {
            double prediction =
naiveBayes.classifyInstance(dataset.instance(i));
            System.out.println("Instance " + i + " risk
probability: " + prediction);
        }

    } catch (Exception e) {
        e.printStackTrace();
    }
  }
}
```

```
CREATE TABLE ai_performance_metrics (metric_id
NUMBER GENERATED BY DEFAULT ON NULL AS
IDENTITY,
   cloud_type  VARCHAR2(30),
   metric_name VARCHAR2(30),
   metric_value NUMBER,
insert_date DATE DEFAULT SYSDATE,
   CONSTRAINT pk_ai_performance_metrics PRIMARY
KEY (metric_id));

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('MultiCloud','Response_Time',12.5);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('Hybrid','Response_Time',10);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('OnPrem','Response_Time',15.75);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('Edge','Response_Time',8.25);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('MultiCloud','Scalability',7.0);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('Hybrid','Scalability',8);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('OnPrem','Scalability',6);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('Edge','Scalability',9);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('MultiCloud','Adaptability',8.5);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('Hybrid','Adaptability',7.75);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('OnPrem','Adaptability',7.0);

INSERT INTO ai_performance_metrics (cloud_type,
metric_name, metric_value)
VALUES ('Edge','Adaptability',9.25);
```

CREATE OR REPLACE PROCEDURE

```
print_avg_response_time IS
   v_multi_avg  NUMBER;
   v_hybrid_avg NUMBER;
BEGIN
   SELECT AVG(metric_value)
     INTO v_multi_avg
     FROM ai_performance_metrics
    WHERE cloud_type  = 'MultiCloud'
      AND metric_name = 'Response_Time';

   SELECT AVG(metric_value)
     INTO v_hybrid_avg
     FROM ai_performance_metrics
    WHERE cloud_type  = 'Hybrid'
      AND metric_name = 'Response_Time';

   DBMS_OUTPUT.PUT_LINE('Average Response Time
for MultiCloud & Hybrid:');
   DBMS_OUTPUT.PUT_LINE('  MultiCloud: ' ||
v_multi_avg);
   DBMS_OUTPUT.PUT_LINE('  Hybrid:     ' ||
v_hybrid_avg);
END;


BEGIN
   print_avg_response_time;
END;
```

Using this study and methodological framework, the scalability and flexibility of artificial intelligence in multi-cloud and hybrid systems may be systematically quantified. By collecting and cleaning data from multiple cloud sources, evaluating key performance indicators, and monitoring system performance in real time, organizations can ensure that their AI-driven solutions remain resilient and adaptable to diverse operating scenarios. This realistic example of PL/SQL code shows how to harvest and analyze such performance indicators on a single database system, supporting data-driven decisions for AI tuning in a cloud cybersecurity setting.

4. Findings

1. AI-driven risk assessment improves the overall detection of anomalies and suspicious activity in cloud environments, allowing for real-time threat detection[14]. Machine learning models can search through mountains of security records for potential attacks faster and more accurately than earlier, rule-based methods.
2. Automation Security Audit powered by AI (Artificial Intelligence) ensures compliance with mandatory compliance requirements (such as ISO 27001, GDPR, HIPAA, and NIST). Reducing manual effort is not only a

way to limit compliance breaches but also to enhance audit efficiency.

3. Now, they can use AI-powered risk assessment to rank security threats by severity. Focusing on the biggest vulnerabilities enables security teams to prevent data attacks before they begin.
4. Even with the differences in platforms, AI models are flexible within multi-cloud and hybrid infrastructure platforms, ensuring continuous security monitoring across machine learning control points.
5. Although this should ensure successful data integration in the early days, the reality is that data handling has not been standardised enough to ensure data integration issues are not chronic in AI.
6. The explainability problem associated with AI-based cybersecurity solutions makes it challenging for security professionals to comprehend AI-generated risk assessments.
7. Improving the model's transparency is vital for building trust and improving decision-making skills.
8. Since cyber threats are constantly changing, security AI models need to be retrained frequently on new cybersecurity datasets. Adaptive AI frameworks that incorporate real-time threat intelligence to improve detection accuracy significantly.

4.1. Suggestions

1. Use explainable AI (XAI) approaches to enhance the interpretability of risk evaluations. Furnish security analysts with detailed explanations of AI decision-making processes.

2. Bring into existence cloud-agnostic AI solutions that work across clouds for compliance auditing across the clouds. Utilize API-based integrations to automate security audits and support real-time compliance automation.
3. Utilize AI-enabled risk-scoring systems to triage and prioritize resources. Create automated response processes for high-risk threats while minimizing interruptions in low-risk efforts.
4. Use new data consistently updated in models from AI systems for cyber threat intelligence. Explore federated learning methods to improve the model's adaptability while preserving data privacy.
5. Implement unified data governance policies that provide cohesion within scalable and AI-enabled security monitoring that spans public, private and hybrid clouds. Focus on data normalization and enrichment to improve the AI model.
6. Use AI-driven automated remediation tools to neutralize security threats before they become crises.
7. Another proactive step cybersecurity services utilize is predictive analytics to identify and eliminate security risks before they become a problem.
8. Share threat intelligence insights and share AI-applied threat intelligence insights and persona-applied threat intelligence insights to overcome evolving cyber threats.

5. Conclusion

AI, which informs risk assessment and compliance automation, offers the potential for cloud cybersecurity, significantly enhancing organizations' ability to identify, monitor, and mitigate cyber risks. The AI approach will outlier and assess threats far more efficiently than traditional methods due to its advanced machine learning algorithms. Risk-based prioritization and key threats can help guide security teams to optimize both resource allocation and reaction times. Furthermore, AI-powered compliance automation ensures that regulatory standards such as ISO 27001, GDPR, HIPAA, and NIST are consistently adhered to, minimizing the risk of non-compliance and accompanying penalties. However, these benefits come with a number of obstacles that need to be fixed.

AI model transparency is a key challenge because security professionals require explainability for AI-driven decisions to build trust and refine incident response strategies. In multi-cloud and hybrid situations, scalability and agility likewise require standardized data governance and seamless AI integration across public and private cloud platforms. As organizations need to be proactive about cyber security, they need to leverage AI to the fullest by creating explainable AI(XAI) frameworks, sharing threat intelligence, and developing AI models that keep learning continuously. Regularly updating AI models with threat information can help strengthen cloud security defences and allow security systems to respond to new cyber threats. Last but not least, an intelligent, scalable, and highly effective approach for cloud cybersecurity is AI-driven risk assessment and compliance solutions. To summarize, AI in Cybersecurity helps organizations adapt to the evolving cyber threat landscape through AI-driven automation, real-time risk assessment, and predictive capabilities – enabling organizations to enhance their security resilience, minimize risks, and ensure compliance with the regulations.

Funding Statement

The authors entirely funded this research.

References

[1] Clémentine Gritti, Willy Susilo, and Thomas Plantard, "Efficient Dynamic Provable Data Possession with Public Verifiability and Data Privacy," *Information Security and Privacy: 20th Australasian Conference*, Brisbane, QLD, Australia**,** pp. 395-412, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[2] Debiao He et al., "Insecurity of an Identity-Based Public Auditing Protocol for the Outsourced Data in Cloud Storage," *Information Sciences*, vol. 375, pp. 48-53, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," *44th Hawaii International Conference on System Sciences*, Kauai, HI, USA, pp. 1-10, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ru Jia et al., "A Systematic Review of Scheduling Approaches on Multi-Tenancy Cloud Platforms," *Information and Software Technology*, vol. 132, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Snehal G. Kene, and Deepti P. Theng, "A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges," *2nd International Conference on Electronics and Communication Systems*, Coimbatore, India, pp. 227-232, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[6] Aiping Li, Shuang Tan, and Yan Jia, "A Method for Achieving Provable Data Integrity in Cloud Computing," *The Journal of Supercomputing*, vol. 75, pp. 92-108, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yongjun Ren et al., "Attributed Based Provable Data Possession in Public Cloud Storage," *Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Kitakyushu, Japan, pp. 710-713, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[8] Wenting Shen et al., "Light-Weight and Privacy-Preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium," *Journal of Network and Computer Applications*, vol. 82, pp. 56-64, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Boyang Wang, Baochun Li, and Hui Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," *Proceedings of International Conference on Applied Cryptography and Network Security*, Berlin, Heidelberg, vol. 7341, pp. 507-525, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[10] Cong Wang et al., "Ensuring Data Storage Security in Cloud Computing in Quality of Service," *Proceedings of WQOS IEEE 17th International Workshop*, vol. 1, pp. 1-9, 2009. [Google Scholar] [Publisher Link]