International Journal of Computer Sciences and Engineering
Vol.**12**, Issue.**7**, pp.**33-40**, July **2024**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Article

Securing Multi-Cloud Environment: An Automated Data Deletion System with Integrated Intrusion Detection System Over Multi-Cloud Platforms

Jashanbir Singh[1*], **Gurjit Singh Bhathal**[2]

[1,2]Dept. of Computer Science and Engineering, Punjabi University, Patiala, India

**Corresponding author: jashanbirpatialvi@gmail.com*

Received: 25/May/2024; **Accepted**: 27/Jun/2024; **Published**: 31/Jul/2024. **DOI**: https://doi.org/10.26438/ijcse/v12i7.3340

Abstract: The recent rapid growth of cloud service providers as more and more users and organizations are moving towards the multi-cloud systems, so that data can be accessed from any part of the world but it poses a humongous problem related to security and privacy of data. Cloud industry needs robust data security system. This research study investigates the feasibility, challenges, and potential impacts of implementing an automated data deletion system, integrated with the capabilities of intrusion detection, in a multi-cloud environment. Through qualitative methods, the aim to understand the experiences, perspectives, and insights of key stakeholders involved in the deployment and operation of such systems. Data collection methods include surveys of focused groups with cloud security experts, IT managers, compliance officers, and developers and an in-depth analysis of existing models and architectures, internal reports, whitepapers, policy documents, compliance guidelines, and security incident records. This research provides an insight and in-depth understanding of the requirements of the individual users and stakeholders of various organizations and improving the overall efficiency of multi-cloud environments by implementing the proposed Automated Data Deletion System with Intrusion Detection System.

Keywords: Cloud Computing, Data Privacy, Data Security, Automated Data Deletion System, Intrusion Detection System

1. Introduction

Cloud Computing have enabled users to upload the data from small amount to huge amount of data from their personal devices and can able to access that data from any part of the world. Other researchers have given the definition of cloud computing as follows Cloud computing [**1**] has enabled data owners to outsource their huge data to the cloud and provided unlimited space in a pay/per-use manner.

The data [**2**] owners are no longer accountable for maintaining and managing their data. In contrast, user queries are handled by the cloud service providers like Amazon, Google, Dropbox, Microsoft but despite its huge advantages, uploading of the data on external cloud services poses quite several security and privacy issues. A multi cloud is proposed to ensure data privacy as data is stored with various different cloud service providers and security. A multi cloud is a cloud which is a combination of public cloud, private cloud, and hybrid cloud but multi-cloud environments pose its own challenges as nowadays, cloud computing [**3**] is popular for various reasons such as increased productivity, speed, efficiency, performance, security, and cost savings. These advantages are achieved because instead of owning their own computing infrastructure, companies can rent a wide range of services like data storage, databases, servers, networking, and software from a cloud service provider. A multi-cloud sends more than one public cloud from various cloud suppliers. A multi-cloud sending can utilize numerous Infrastructure-as-a-Service (IaaS) merchants, or it could utilize an alternate seller for IaaS, Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) administrations.

Using multi- cloud has its own advantages but it also comes with various data security and privacy issues as mentioned in the report [**3**] there also exists possibility of greater challenges for service quality, security, and privacy attacks. This chapter presents an attempt to elaborate various algorithms used for the security of data and to provide quality service.

As author of [**4**], highlighted that data accountability and integrity is a significant challenge in multi-cloud with limitations being restricted to the tier 1 Cloud Service Providers and a need for consistent benchmarking or framework across private industry and public sector alike.

As a result, with multi-cloud security solutions, enterprises are better equipped to protect against modern threats. The lack of interoperability is a root cause of security issues in multi-cloud environments, as seen in the incident at Uber in September 2022. The attack compromised the company's multi-cloud setup by accessing an admin username and password stored in PowerShell scripts for automation. The same username and password gave the attacker access to all cloud services at Uber. This example underscores the importance of implementing robust security measures, including secure access management, and the need for an integrated approach to multi-cloud security that addresses the unique security capabilities and features of individual providers while ensuring interoperability across all providers [**5**].

Data privacy and security issues [**6**] can be solved by establishing clear policies that enable authorised data access and security. Outsourcing the data to the cloud servers signifies that the data is out of the users' control resulting in discomfort to the users because the outsourced data may comprehend sensitive and valuable information. Data sharing is frequently put into operation in a hostile and open environment, and the cloud server turned out to be a target of attacks. In the worst condition, users' data may be revealed by the cloud server itself for illegal profit [**7**] [**8**].

2. Literature Review

In the paper given by Pan Jun Sun, he mentioned about data privacy and security issues [**9**]. Furthermore, in paper given by Kire Jakimoski, he mentioned that Protection of data [**10**] in the cloud is best accomplished when there is a mixture of encryption, data loss prevention techniques, integrity protection, authentication, and authorization techniques.

When vendors and enterprises use cryptographic algorithms, it is very important these algorithms to be well known as identified by NIST. It is also useful to have re-evaluation on an annual basis of the algorithms and keys that are utilized in order to be assured about the strength of the protection.

In all the papers which we read, mentioned security of data is always ignored in a multi cloud environment. Existing multi-cloud architectures have security issues on cloud platforms was manifested in a paper [**11**] published by Deepika Saxena, Rishabh Gupta, and Ashutosh Kumar Singh. The existing strategies and architectures (proposed by several different researchers) have some strengths and weaknesses, which is mentioned below in a tabular form: in table 1 strategies and architectures and in table 2 we mentioned the strength and weakness of the existing models.

Table 1: existing strategies and architectures

Model, Researcher/es	**Aim**
CHARM (Zhang et.al, 2015) [**12**]	Cost-efficient multi cloud data hosting mechanism where availability is the main priority. [**11**]
EGI FEDERATED CLOUD [**15**]	EGI Federated cloud integrates public, private or hybrid cloud in the form of multinational cloud system. [**11**]
DISTRIBUTED MANAGEMENT TASK FORCE(DMTF) ARCHITECTURE (Paper et al.,2009) [**13**]	Open Cloud standards Incubator models for enabling interoperability in multi-cloud environment. [**11**]
RESERVOIR MODEL (Rochwerger et al., 2009) [**14**]	Reservoir model for federated cloud computing. [**11**]
Cloud Foundry [**16**]	It aims to provide a standardized platform to the applications of customers by decoupling the application from its infrastructure. [**11**]

In the above table 1: existing strategies and architectures, and in table 2, we mentioned strength and weakness of the existing models, we have mentioned some of the existing strategies and architectures. Let us discuss these models in little bit more detail, the CHARM model aimed to be cost effective multi-cloud data hosting model. In this data will be stored at different locations in a cost-effective manner but it poses the biggest challenge of security of the data. In EGI federated cloud, we can see it is a combination of public, private and hybrid cloud. In this user can access the services of the cloud under single identity but it can lead to lack of trust and security issues. In Distributed management task force architecture, provides interoperability in multi-cloud platforms, this model also lacks trust and reliability between the users and security is also the main concern. In reservoir model, which is also a federated cloud model but still security is the major concern in this model which authors did not talk about. In the last model which is mentioned above in the table 1, is cloud foundry, it's main goal is to provide a standardized platform for the implementation of the applications. In this model, it all depends on the sole description of the business stakeholders that where to distribute the workload of the cloud system but this model does not deal with handling of the data in a proper way, it also lacks security issues. It is clearly evident from the above that all the already existing strategies and architectures lacks in security. It poses a great challenge for the stakeholders to design and develop a system ensuring data integrity and security.

Table 2: Strength & Weaknesses of Models

Strength	**Weakness**
CHARM (Zhang et.al, 2015) [12]	
It provides guidance to the customers to distribute their data on multiple clouds in cost effective manner. [**11**]	Security is the main concern in this model. [**11**]
EGI FEDERATED CLOUD [15]	
User can access all services of cloud federation with a single identity. [**11**]	Federated cloud Model lacks trust & unauthorized access issues and other security features not considered. [**11**]
DISTRIBUTED MANAGEMENT TASK FORCE (DMTF) ARCHITECTURE (Paper et al., 2009) [13]	
They have conceptually provided Incubator models for handling interoperability in multi-cloud environment. [**11**]	Service Provider is unaware of this resource provisioning. So, lack of reliability and trust. Security is major concern that is not included here. [**11**]
RESERVOIR MODEL (Rochwerger et al., 2009) [14]	
The resource usage optimization at each reservoir site. Interoperability is handled by VEE management interface that supports VEEM-to-VEEM Communication. [**11**]	Security, access feature, management of various multi-cloud architecture are not discussed. The practical implementation of this reservoir model is not given. [**11**]
Cloud Foundry [16]	
The organizations can easily make a business decision on where to deploy workloads i.e. on premise, in managed infrastructure. [**11**]	This model does not handle load balancing, security and data storage handling issues. [**11**]

By looking at the above tables: table 1 and table 2, we can say that most of the models, architectures which are proposed till now have data security issues.
The security of cloud computing [**19**] is a critical issue, and among the various challenges, cloud data security has gained significant attention due to the crucial role of data in cloud computing and its increasing adoption in various domains. The storage and processing of sensitive data on the cloud raise concerns about the confidentiality, integrity, and availability of data. As a result, several security measures have been developed, including encryption, access control, and intrusion detection systems (IDS).

Recent research [**19**] has highlighted the importance of enhancing the effectiveness and efficiency of intrusion detection systems (IDS) for cloud data security.
As cloud computing continues [**19**] to grow and evolve, the use of IDS in cloud data security is becoming increasingly important in mitigating cyber threats and ensuring the privacy and security of sensitive data. Generally, there are two primary types of IDS: host-based IDS (HIDS) and network-based IDS (NIDS).

The current research, focuses on machine learning algorithms, has significantly improved the capabilities of IDS, cloud data security still faces various challenges, particularly in multi-cloud environments. Machine learning algorithms can help IDS identify complex attacks and malicious activities that were previously difficult to detect [**20**]. However, [**19**] the effectiveness of these algorithms can be limited by the quality of the training data and the ability to identify new and unknown threats. In addition, multi-cloud environments pose a unique challenge for cloud data security, as they involve multiple cloud service providers and require the coordination of various security protocols. In such environments, the complexity of managing and securing data across multiple clouds can create vulnerabilities that can be exploited by attackers. Therefore, cloud service providers and their clients must continue to develop and implement effective security measures to protect sensitive data in multi-cloud environments.

The research conducted by author of [**20**] and [**18**] presents a collaborative network security prototype system, vCNSMS, designed for a multi-tenant data centre to protect against potential network attacks.
It is clearly evident that stakeholders are suffering from a grave problem related to data security in multi-cloud environments. As we can see the director of cloud security at Microsoft clearly stated that existing systems are not capable enough to handle security issues in multi-cloud environment. It further motivated me to develop an integrated system, which can deal with the security issues in whole which further leads to automated data deletion system with integrated intrusion detection system.

3. Research Methodology:

3.1 Introduction:

Objective: The goal of this research is to create the blueprint, implementation, and to assess an automated data deletion system with intrusion detection system integrated into it for multi-cloud environments. In this proposed system will respond to the intrusion detection alerts.
Scope: The system may cover well renowned cloud platforms like AWS, Azure, and Google Cloud Platforms, concentrating on the secure data deletion, compliance logging and ensuring data integrity and confidentiality.

3.2 Literature review:

Purpose: To get the insight of the working and implementation of the already existed methods and technologies related to the deletion of the data, multi-cloud environments, implementation of the clouds and intrusion detection system.
Reviewing research papers, whitepapers, and case studies on automated data deletion mechanisms. Analysis of the current practices and the obstacles and limitations in intrusion detection systems. Studying the compliance requirements (like GDPR, CCPA, HIPAA etc.) related to data deletion and secure management of the data. Different regions have different compliance requirements.

3.3 System design: In this development of architecture will take place:

Setting up multi-cloud: designing a robust architecture of the system that supports AWS, Azure and Google cloud. This may include various tasks like configuring the virtual machines, storage solutions and access management.
Integration of IDS Intrusion Detection System: detection of security breaches, system will integrate AWS GuardDuty, Azure Security Centre and Google cloud security command center.
Data deletion engine: Developing the data deletion engine with deletion interfaces and a controller. This interface will be unique for AWS, Azure, Google cloud platforms.
Monitoring module: this module will maintain all the logs and monitor all the activities related to the data deletion.

The automated system consists of various components and we may need to create a detailed design of each component like data flow diagrams, in this it will be explained that how the system will proceed from starting to the end of data deletion. Prototyping is also a required step to ensure that proposed system will be effective in data deletion. It further leads to initial testing of the system as it is necessary to evaluate the system before its implementation.

3.4 Implementation:

Establishing an environment setup:
AWS, Azure, Google cloud needed to be configured properly with necessary services like virtual machines, storage units, and security settings.
Setting up IDS Intrusion Detection System in each cloud environment. We need to configure IDS to track the alerts and triggers, effectively in a cloud.
Data Deletion Engine Development is needed to be developed for each cloud platform which can be done by writing python scripts for the secure deletion of the data. For every cloud platform there is a different service mentioned below in table 3 below:

Table 3: Cloud platform & Service

Cloud Platform	Service
AWS	Boto3
Azure	Azure-storage-blob
Google Cloud	Google-cloud-storage

3.5 Logging and monitoring: implementation of the logging mechanism is necessary for audit purposes. If any error occurred in the system, it will be analyzed and fixed by studying the logs. The cloud platforms and the monitoring of the platforms mentioned in the table 4 below:

Table 4: Cloud platform & Monitoring

Cloud Platform	Monitoring
AWS	AWS CloudWatch
Azure	Azure Monitor
Google Cloud	Google Cloud Monitoring

3.6 Testing and validation:
Testing individual components like python scripts, integration of various modules like IDS, data deletion engine to ensure its proper functionality and it is necessary to check that all the components of proposed automated data deletion system with integrated intrusion detection system are working properly and well integrate with each other for a robust system.
Penetration testing will be done simulate the intrusions and check the response of the proposed system.

As different regions of the world having different laws and compliance requirements governing the management of the data. It is necessary to ensure the proposed data deletion system follows the laws and requirements of GDPR, HIPAA and CCPA.

3.7 Evaluation:
Metrics like response time of data deletion engine. It will help the stakeholders to analyze the accuracy of intrusion detection and the data deletion mechanism.

3.8 Result and Analysis:
For the security of the data, we proposed an automated data deletion system with integrated intrusion detection system, will be compared with existing methods and systems in the following areas:

3.8.1. Existing Data Deletion Methods:
Data deletion is the process of deleting the data.
Manual Deletion Processes: conventionally, deletion of the data in cloud environments, done manually. It is a laborious task and time-consuming.
Automated Deletion Systems: Existing automated data deletion systems lacks integration of intrusion detection or multi-cloud capabilities.

3.8.2 Intrusion Detection Systems (IDS) Integration
Standalone IDS Solutions: Systems that detect intrusions but do not trigger automatic data deletion.
Integrated Security Solutions: Security solutions that provide some level of integration between IDS and data management but may not cover multi-cloud environments.

3.8.3 Compliance and Security Standards
Compliance Mechanisms: Compliance frameworks are followed and their effectiveness in ensuring data deletion meets regulatory standards.
Security Protocols: Security measures in place for current data deletion practices compared to the proposed system's comprehensive security testing and validation.

3.8.4 Performance and Scalability
Performance Metrics: Speed and efficiency of data deletion in response to intrusions in current systems versus the proposed system.
Scalability: Ability of existing systems to handle increased loads and simultaneous alerts compared to the proposed system’s scalability.
Thus we can finally conclude that these combined approaches which we decided to use, ensured that the research methodology which was chosen is vigorous, transparent, and credible for the proposed automated data deletion system with integrated intrusion detection system.

4. Proposed Work

In this research, we proposed a development of an exhaustive system for automated data deletion in a multi-cloud environment with the capabilities of Intrusion detection. The proposed system aims to address the complex challenges associated with managing data privacy and security across multi-cloud infrastructures. The key components of the system include a policy driven data deletion mechanism, an intrusion detection system tailored for multi-cloud architectures, and a centralized policy engine for defining, evaluating, and enforcing policies governing data deletion, access control, and compliance.

Our approach leverages policy-based management techniques to enable dynamic and flexible enforcement of data deletion policies, ensuring adherence to regulatory requirements and organizational policies. By integrating intrusion detection capabilities, the system enhances security posture and enables proactive identification and response to security threats and anomalies. Through this research, the aim is to contribute to the advancement of data management practices in multi-cloud environments and provide organizations with effective tools and methodologies for ensuring data privacy, compliance, and security in the cloud.

4.1 Automated data deletion system with integrated intrusion detection system in multi cloud
There are various existing models available which deals with data privacy and security in multi-cloud environment, some of the models which, we studied in our literature review, we found that existing models and techniques deals with data privacy and security with one sided approach but no researcher have tried to design a system which directly deletes data in an event of an attack like ransomware attack, distributed denial of service attack etc. in our system data gets deleted as soon as any intruder try to get a hold on to the data for malicious purposes. Automated Data Deletion System consists of several components namely,

4.1.1 Policy engine:
It is the main component of proposed system, through this engine (as seen in figure 1), organisations and institutions can define manage data deletion policies based on their unique

requirements and compliance with the regulatory can be maintained. Policy engine plays a vital role as it handles the whole mechanism of proposed system. It also manages compliance checks of various regulations like GDPR, CCPA and HIPAA. Policy engine is an integral part of the our proposed data deletion system with integrated intrusion detection system.

4.1.2 Data Deletion Engine:
It will consist of various components like Intrusion Detection Trigger, which constantly listening to the alerts from the Intrusion Detection System indication a breach to the security of the data. It also consists of Data Deletion Controller which will actually initiate the deletion of the data. Data deletion engine and policy engine works hand in hand which means the changes which we will do in policy engine will directly reflects in data deletion engine. It executes the deletion of data based on the defined policies in the policy engine. Data deletion engine (as seen in figure 1), directly works with cloud APIs to delete data from multiple cloud environments.

4.1.3 Intrusion Detection System:
This component (as seen in figure 1), will actively monitor the multi-cloud environments for any malicious attempt and any other suspicious activity. As soon as it got detected, intrusion detection system will immediately send the interrupt to policy engine which further orders the data deletion engine to securely delete the data instantly so that malicious entity cannot able to get the hold on to the data. In this detection time of the intrusion will directly affect the response time to trigger the deletion of the data.

4.1.4 Cloud APIs:
This component (as seen in figure 1), directly interacts with cloud service providers (like AWS, Google Cloud) to interact with data storage servers and execution of data deletion. Cloud APIs ensures interoperability and management among multi-cloud platforms while minimizing the complexity and vendor lock-in.

4.1.5 Logging and Monitoring:
This component (as seen in figure 1), stores all the audit logs, system metrics, intrusion alerts, compliance checks and all the other components related to proposed automated data deletion system. This component will provide graphical user interface to all the stakeholders, i.e. organizations and authorised users, they all can access this interface to have an insight. This can be achieved by log aggregators like Logstash, Elasticsearch.

4.1.6 Reporting and Dashboarding:
This component (as seen in figure 1), generates reports and provide the dashboard to visualize system performance, compliance status, and all the data deletion operations. It helps all the stakeholders to track the system to have an insight. The above proposed architecture enables the automated data deletion system to manage the whole lifespan of data across different multi-cloud platforms, enforces data deletion policies and ensure compliance with all the regulatory requirements. Every component plays their unique role in overall functionality of our proposed automated data deletion system and contributes to protect sensitive data in a multi-cloud environment.

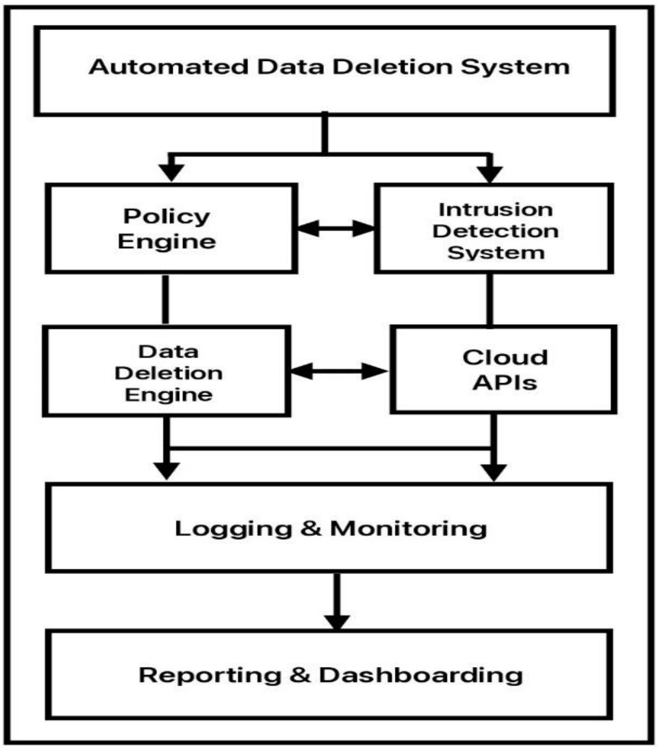

Figure 1: Proposed Automated Data Deletion System

The Automated Data Deletion System with Intrusion Detection System can be implemented in different sectors, like financial systems, e-commerce platforms, academic institutions. Let us discuss one of the systems in detail,

5. Results and Discussion:

In this part, we are presenting out findings of our study on the security and privacy issues associated with multi-cloud environments. In this the in-depth discussion and why our automated data deletion system with integrated intrusion detection compared to state-of-the-art techniques related to data privacy and security, presented in previously published reports, highlights the novelty of our work through comparative analysis with existing literature. We will discuss our results in detail below:

5.1 Existing Data Deletion Methods:
Data deletion is the process of deleting the data.
Manual Deletion Processes: as discussed by [author of 3] that cloud platforms are suffering from data security and privacy risks and in order to overcome that we need robust system. As we see in literature that conventionally, deletion of the data in cloud environments, done manually. It is a laborious task and time-consuming. Automated Deletion Systems: Existing automated data deletion systems lacks integration of intrusion detection

5.2 Intrusion Detection Systems (IDS) Integration
Existing IDS Solutions: as discussed by [author of 19 and 20], that we need to intrusion detection systems to mitigate cyber threats, IDS can detect intrusions but do not trigger automatic data deletion.

Integrated Security Solutions: Security solutions that provide some level of integration between IDS and data management but may not cover multi-cloud environments.

This research study, employed a comprehensive approach in identifying and reduce the data security vulnerabilities specific to multi-cloud platforms. Unlike some previous studies that focused on data security.

Multi-cloud platforms are established in a complex manner, as the storage units are installed at different sites increases the chance of data breaches and malicious entities try to gain unauthorized access. Security gaps in authentication mechanisms, misconfigured permissions, and inadequate encryption practices pose significant risks to data confidentiality and integrity.

The proposed automated data deletion system with integrated intrusion detection in a multi-cloud environment can be assessed through the following aspects:

5.3 Conceptual Framework

Security and Compliance Frameworks: The proposed automated data deletion system with integrated intrusion detection is outlined based on the accepted security and compliance frameworks such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) and HIPAA (Health Insurance Portability and Accountability Act). These existing and widely accepted frameworks consists of stringent data protection and deletion practices, providing a strong theoretical basis for the necessity and outline of the system.

Zero Trust Security Model: as mentioned by the [author of 17] that it requires users and services to verify their identity credentials [**17**] before accessing corporate cloud resources. In this way, access to critical resources becomes more secure. Our model is adapted to modern cloud storage systems and makes user data more secure, in line with the famous quote “Never trust, always verify”. The system aligns with the Zero Trust Security Model, which assumes that threats are omnipresent both inside and outside the network. By automatically deleting data upon detecting an intrusion, the system ensures that sensitive information is not compromised, supporting the Zero Trust principles.

5.4 Data Lifecycle Management

Data Lifecycle Management (DLM): It is a unique approach for gathering of the data to its complete management of the data to the phase where data is no longer needed. The proposed system brings the automation in the management of the data and the system also integrated with the principles of DLM - Data Lifecycle Management. By automatically deleting data upon the detection of threats, the proposed system ensures that data is managed and protected throughout its lifecycle.

5.5 Intrusion Detection and Response Theory

Automated Response Systems: The design of the proposed system is embedded in the mechanism of automated response systems, which focuses on the need for immediate reacting to the security threats automatically and mitigating the potential damage.

Event-Driven Architecture: The proposed system follows an event-driven architecture where detection of the intrusion going to trigger a pre-defined automated response (data deletion). This theoretical approach ensures quick, timely and efficient handling of security incidents.

5.6. Fault Tolerance

Fault Tolerance Theory: As its name suggests, it deals with the tolerance of the fault in the system. The proposed system is designed to function and operate in a fault-tolerant manner. It greatly ensures that the process of data deletion is reliable and resilient to failures. This will provide a strong theoretical base for the system's robustness.

5.7 Compliance and Auditability

Compliance Models: The system incorporates compliance models that ensure all actions are logged and auditable, providing a theoretical basis for meeting regulatory requirements and facilitating transparency and accountability.

Regulatory Compliance: By adhering to data protection regulations, the system theoretically validates its capability to operate within legal frameworks, thus enhancing its credibility and reliability.

5.8 Summary: The proposed automated data deletion system with the integration of intrusion detection system in a multi-cloud environment is theoretically validated through its proper calibration with already established data deletion mechanism, intrusion detection systems, security and compliance frameworks, data lifecycle management principles, automated response systems, fault tolerance theory, and compliance models. This theoretical foundation guarantees that the proposed system is designed to be secure, compliant, and efficient, providing a robust solution for protecting confidential and sensitive data in multi-cloud environments.

5.9 Use Cases:

Following are the two use-cases in which we can implement our proposed automated data deletion system with integrated intrusion detection system:

5.9.1 Healthcare Network:

Scenario: The network of health care providers like clinics, hospitals collaborate together on patient care and medical research, storing all the sensitive and confidential data of the patients in the multi-cloud environments. Patient privacy is very important and crucial for any healthcare network and in order to protect patient privacy and comply with Health Insurance Portability and Accountability Act (HIPAA) regulations, the network must implement strong data management practices and privacy measures to protect the data from malicious entities and timely data deletion of records of the patients so that malicious entities cannot able to access the data of patients.

Solution: Deploying an automated data deletion system across multi-cloud environment to manage the lifespan of the patient’s data. Our proposed system will delete the patient’s data when it is no longer needed so that privacy can be ensured. Integration of Intrusion Detection capabilities to monitor the security incidents and potential data breaches.

Implementation of strong authorization strategies and encryption policies on data both at rest and in transit. The proposed automated data deletion system with intrusion detection system enables us to delete data, mitigating data breaches and maintain great trust in between patients, healthcare network and stakeholders. Thus, it validates the need of our proposed automated data deletion system with integrated intrusion detection system.

5.9.2 E-commerce Network

Scenario: The network of e-commerce service providers like Amazon, Flipkart stores the data of the customers on different servers around the globe. On different servers, companies store all the sensitive and confidential data of the customers like transaction details, home addresses of the customers, and contact information of the customers in the multi-cloud environments. Customer data security and privacy is very important and crucial for any e-commerce network and in order to protect customer privacy and comply with Digital Personal Data Protection Ac (DPDP or DPDPA Act), the network must implement strong data management practices and privacy measures to protect the customer data from malicious entities and timely data deletion of records of the patients so that malicious entities cannot able to access the data of the customers. The DPDP Act mandates the e-commerce platforms to delete the data of the customers who are inactive for 2-3 years. Deletion of the data of the inactive users helps the organisation to maintain data integrity and security.

Solution: Deploying an automated data deletion system across the servers of an e-commerce platform to manage the lifespan of the customer's data. Our proposed system will delete the customer's data when it is no longer needed so that privacy can be ensured. Integration of Intrusion Detection capabilities to monitor the security incidents and potential data breaches. Implementation of strong authorization strategies and encryption policies on data both at rest and in transit. The proposed automated data deletion system with intrusion detection system enables us to delete data, mitigating data breaches and maintain great trust in between customers, e-commerce network and stakeholders. Thus, the proposed system ensures that the sensitive information of the customer is protected, which will establish the trust between customers. Thus, it validates the need of our proposed automated data deletion system with integrated intrusion detection system.

6. Conclusion and Future Work

Our study on data security, integrity, and protection of the data gained deeper insights that advanced our knowledge and deeper understanding of the threats, risks and issues related to the integrity and security of the data. Our deeper research and analysis helped us in identifying the weaknesses into current existing systems and lack of proper data management systems as discussed by the authors references included in the literature survey. It further, paved a way for us to align our proposed automated system with the needs of data deletion mechanism, intrusion detection systems, security and compliance frameworks, data lifecycle management principles, automated response systems, fault tolerance theory, and compliance requirements like GDPR, DPDP or DPDPA, CCPA and HIPAA.

The proposed system is calibrated with the Zero Trust Security Model and Data Lifecycle Management which ensures a vigorous approach to the protection of the data. As the intruder can be internal or external, by employing the zero-trust model, users are ensured that their data is protected and secured. Further, with the implementation of event-driven architecture into our proposed system triggers the immediate deletion of the data as soon as intrusion is detected, thus protecting the multi-cloud from data breaches.

Our work is novel because it deals with integrity and security of the data with included intrusion detection system which deals with data breaches. We proposed a new autonomous system named as ADDS-IDS, Automated Data Deletion System with integrated Intrusion Detection System. Our study shows the importance of data security and data integrity measures in multi-cloud environments.

To sum up, the proposed system ensures the security of data over multi-cloud platforms. Our research increases the confidence of a user that his/her data will be secured in multi cloud environment which prompts them to use cloud services instead of those conventional systems. The proposed system deletes the highly confidential data in an event of data breach by trigging the data deletion engine which works on predefined policies in the policy engine and this automated data deletion system with intrusion detection system further omits the possibility of any data breach.

As for future work, the proposed system can be enhanced by exploring the techniques of machine learning to increase the capabilities of IDS – intrusion detection system and development of a user-friendly graphical user interface to manage the automated system.

Conflict Of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper. No external funding or support from commercial organizations was received for the research, authorship, and publication of this study. All opinions, findings, and conclusions presented in this paper are solely those of the authors and are based on their independent research. The authors have no affiliations or financial involvements with any organization or entity with a direct interest in the subject matter discussed in this manuscript.

Funding Source

No, external funding or supporting grants from any commercial organizations was received for this research, authorship, and publication of this study.

Author's Contribution

Author-1 researched literature and conceived the study, wrote the first draft of the manuscript.

Author 2-involved in protocol development, gaining ethical approval, and data analysis. manuscript.

All authors reviewed and edited the manuscript and approved the final version of the manuscript.

Acknowledgement

We would like to express our sincere gratitude to all those who supported us throughout this research. first and foremost, we like to thank Dr. Gaurav Gupta and Dr. Brahmaleen K Sidhu, our advisors, for their invaluable guidance, insightful feedback, and continuous encouragement. Their expertise and dedication have been instrumental in shaping the direction and outcome of this study.

We also extend our token of appreciation to Department of Computer Science and Engineering, Punjabi University, Patiala, India for providing the necessary resources and a conducive environment for conducting this research. The technical support and facilities offered by the institution were essential in achieving our objectives.

Special thanks to our colleagues and fellow researchers for their collaborative spirit and constructive discussions, which significantly contributed to the development of this paper.

Finally, we are grateful to our families and friends for their unwavering support and understanding throughout this journey. Their patience and encouragement were crucial in helping us to stay focused and motivated.

References

[1] Blesson Varghese and Rajkumar Buyya. 2018. Next generation cloud computing. Future Gener. Comput. Syst. 79, P3 (Feb.), pp.**849–861, 2018**. https://doi.org/10.1016/j.future.2017.09.020

[2] Yang, P., Xiong, N., Ren, J., **2020**. Data security and privacy protection for cloud storage: A survey. IEEE Access **8**, **131723–131740**. Yu, Y. et al., **2016**. Identity-based remote data integrity checking with perfect data DOI: https://doi.org/10.1109/ACCESS.2020.3009876

[3] Kavitha, M.G., Radha, D., Quality, Security Issues, and Challenges in Multi-cloud Environment: A Comprehensive Review. In: Nagarajan, R., Raj, P., Thirunavukarasu, R. (eds) Operationalizing Multi-Cloud Environments. EAI/Springer Innovations in Communication and Computing. Springer, Cham. **2022.** https://doi.org/10.1007/978-3-030-74402-1_15

[4] Spencer, K., Withana, C., Exploring Cyber Security Challenges of Multi-cloud Environments in the Public Sector. In: Mukhopadhyay, S.C., Senanayake, S.N.A., Withana, P.C. (eds) Innovative Technologies in Intelligent Systems and Industrial Applications. CITISIA **2022**. Lecture Notes in Electrical Engineering, Vol.**1029, 2023**. Springer, Cham. https://doi.org/10.1007/978-3-031-29078-7_19

[5] Morgan Reece, Theodore Edward lander, Matthew stoffolano, Andy Sampson, Josiah Dykstra, Sudip Mittal, Nidhi Rastogi Systemic Risk and Vulnerability Analysis of Multi-cloud Environments, **2023**. DOI: https://doi.org/10.48550/arXiv.2306.01862

[6] S. Kanaga Suba Raja, A. Sathya, S. Karthikeyan, and T. Janane Multi cloud-based secure privacy preservation of hospital data in cloud computing, Vol.**10, 2021.** https://doi.org/10.1504/IJCC.2021.113993

[7] I. Gupta and A. K. Singh, "Dynamic threshold-based information leaker identification scheme", *Inf. Process. Lett.*, Vol.**147**, pp.**69-73**, **2019**. DOI: https://doi.org/10.1016/j.ipl.2019.03.005

[8] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing", *IEEE Trans. Inf. Forensics Security*, Vol. **11**, No.**6**, pp.**1265-1277**, **2016**. DOI: https://doi.org/10.1109/TIFS.2016.2523941

[9] Pan Jun Sun Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions, Vol.**7**, **2019.** DOI: 10.1109/ACCESS.2019.2946185

[10] Kire Jakimoski Security Techniques for Data Protection in Cloud Computing International Journal of Grid and Distributed Computing Vol.**9**, No.**1**, pp.**49-56, 2016.** doi: http://dx.doi.org/10.14257/ijgdc.2016.9.1.05

[11] Deepika Saxena, Rishabh Gupta and Ashutosh Kumar Singh A SURVEY AND COMPARATIVE STUDY ON MULTI-CLOUD ARCHITECTURES: EMERGING ISSUES AND CHALLENGES FOR CLOUD FEDERATION arXiv:2108.12831v1 [cs.DC] **29 Aug 2021.** DOI: https://doi.org/10.48550/arXiv.2108.12831

[12] Q. Zhang, S. Li, Z. Li, Y. Xing, Z. Yang, and Y. Dai, "Charm: A cost-efficient multi-cloud data hosting scheme with high availability," IEEE Transactions on Cloud computing, Vol.**3**, No.**3**, pp.**372–386**, **2015**. DOI: https://doi.org/10.1109/TPDS.2023.3306150

[13] I. Clouds, "A white paper from the open cloud standards incubator," Distributed Management Task Force, Version, Vol.**1, 2009**.

[14] A. Galis, E. Elmroth, W. Emmerich, F. Galán, and S. Telefónica, "The reservoir model and architecture for open federated cloud computing," IEEE Computer Society Press, Vol.**20**, pp.**115–187, 2009**.

[15] E. Fernández-del Castillo, D. Scardaci, and Á. L. García, "The egi federated cloud e-infrastructure," Procedia Computer Science, Vol.**68**, pp. **196–205**, **2015** DOI: https://doi.org/10.1016/j.procs.2015.09.235

[16] D. Bernstein, "Cloud foundry aims to become the OpenStack of paas," IEEE Cloud Computing, Vol.**1**, No.**2**, pp.**57–60**, **2014**. DOI: https://doi.org/10.14738/tmlai.54.3334

[17] M. E. Moudni and E. Ziyati, "A Multi-Cloud and Zero-Trust based Approach for Secure and Redundant Data Storage," *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Istanbul, Turkiye, pp.**1-6**, **2023.** doi: 10.1109/WINCOM59760.2023.10323009.

[18] Z. Chen, F. Han, J. Cao, X. Jiang and S. Chen, "Cloud computing-based forensic analysis for collaborative network security management system," in Tsinghua Science and Technology, Vol.**18**, No.**1**, pp.**40-50**, Feb.**2013**, doi: 10.1109/TST.2013.6449406.

[19] Zhang, X., Cui, L., Shen, W. *et al.* File processing security detection in multi-cloud environments: a process mining approach. *J Cloud Comp* **12**, **100, 2023.** https://doi.org/10.1186/s13677-023-00474-y

[20] Li J, Tong X, Liu J, Cheng L., An efficient federated learning system for network intrusion detection. IEEE Syst J. **17(2):2455-64, 2023.** DOI:10.1109/JSYST.2023.3236995

[21] Chiba Z, Abghour N, Moussaid K, Rida M et al., Intelligent approach to build a deep neural network based ids for cloud environment using combination of machine learning algorithms. Comput Secur **86:291–317, 2019.** doi: https://doi.org/10.1016/j.cose.2019.06.013

AUTHOR'S PROFILE

Jashanbir Singh received his B.Tech. degree in Computer Science and Engineering from Punjabi University, Patiala in 2020 and is currently pursuing his M.Tech degree batch 2020, He is active researcher in the field of Cloud Computing including Cloud Security, Data Security and Privacy and Intrusion Detection System.

Dr. Gurjit Singh Bhathal is currently working as an Assistant Professor (Senior Scale) in Department of Computer Science and Engineering, Punjabi University, Patiala (Pb). He has received Ph.D. in Faculty of Engineering and Technology and, M.Tech. in Computer Science and Engineering from Punjabi University. He did his B.Tech. in Computer Science and Engineering from SLIET, Longowal, India. He has more than 24 years of experience in teaching and industry in India and abroad. He has supervised more than 39 M.Tech. dissertations. Besides contributing to more than 98 publications in various reputed international journals and participating in many international conferences. He has authored 5 books. His research interests include Big Data, Cloud Computing, Information Security, Cyber Security, and Data Analytics. He is a member of IAENG, ICSES, and CSI. He is on the editorial board of various journals. He, along with a team of his students, completed two projects for Punjabi University. Dr. Bhathal was also **awarded an Outstanding Scientist in Computer Science and Engineering at 4th Annual Research Meet – 2018** and is listed in "**100 Eminent Academicians of 2021**" by International Institute of Organized Research.