An Automated Data Deletion: A Secure Method for Multi-Cloud Security with Intrusion Detection System

Jashanbir Singh[1], Dr. Gurjit Singh Bhathal[2]

[1]Department of Computer Science & Engineering, Punjabi University, Patiala, Punjab, India
Corresponding Author Email: *jashanbirpatialvi[at]gmail.com*

[2]Assistant Professor, Department of Computer Science & Engineering, Punjabi University, Patiala, Punjab, India
Email: *gurjit.bhathal[at]gmail.com*

Abstract: ***Since the outbreak of Covid-19, there is a rapid boom in adoption of online cloud services as users are using online platforms to but all the necessities, it prompted the companies to move to multi-cloud platforms to store and manage the data of products and customers. But cloud-platforms are lagging in providing data security and privacy as proper mechanisms has not been developed till now. In a matter of time an intruder can get the access of the data which is stored over multi-cloud platforms. There is a need of a robust system which deletes the data as an intruder try to get hold on to the data for malicious reasons. In this paper, we proposed a brief idea of the unique system who deletes the data as soon as intrusion happens. We named the system as Automated Data Deletion System with Integrated Intrusion Detection System. ADDS-IDS system may have the capability to revolutionize the multi-cloud industry as it provides a quick and unique way to deal with the data breaches.***

Keywords: Cloud Computing, Data Security, Intrusion Detection System, Data Deletion System, Automation

1. Introduction

Cloud Computing opened a new realm for the users worldwide as it provides a way to the users to access the services provided by the cloud service providers with the help of internet and a display unit. Users can upload, manage, modify, and delete the data as per their choice. Users can also access wide range of services provided by the CSPs (cloud service providers). 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 on different servers. The servers can be installed at different locations, nationally or internationally and through this data security can be ensured but the data ca still be accessed by the malicious entities. 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.

Using multi- cloud has its own advantages but it also comes with various data security and privacy issues as discussed by the researcher in [**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. Data privacy and security issues [**6**] can be solved by establishing clear policies that enable authorised data access and security. Over the period, many researchers have proposed different systems and models to enable the data privacy and security but no mechanism is sufficient in string enough to ensure the privacy and security of the data as still 76% of the entities are concerned by the cloud security.

2. Literature Survey

Researcher, Pan Jun Sun, explained about data privacy and security issues [**4**]. Even after several models and systems and architectures proposed by the different researchers and organisations, over the period of time but no one model is capable enough to provide security to the data and helps in maintaining data security. Further, in paper given by Kire Jakimoski, he raised that Protection of data [**5**] in the cloud is best accomplished when there is a mixture of encryption, data loss prevention techniques, integrity protection, authentication, and authorization techniques. In the papers, which we surveyed, mentioned data security and privacy is always overlooked in a multi-cloud environment as it is difficult to develop a unique system and implement it over multi-cloud environment.

As moreover, we can see that existing available models and architectures that deals with the implementation of cloud services consists of several security issues on cloud platforms mentioned in the paper [**6**] given by Deepika Saxena, Rishab Gupta and Ashutosh Kumar Singh.

The models consist of different strengths and weaknesses mentioned in the tabular form given below in table 1 and table 2: in table 1, we mentioned about model and its aim and in table 2. In this we will talk about various models and architectures that deals with the implementation of cloud

Paper ID: SR24730194843 DOI: https://dx.doi.org/10.21275/SR24730194843

services and we talked about strengths and weaknesses of the models and architecture.

By the table number 1 and table number 2, given below, we can see the model Charm which is a cost-effective model. It hosts data in clouds but it lacks in security. In the model named as EGI Federated Cloud, in this private, public and hybrid cloud are combined together to form a multi-national cloud systems but this model lacks trust issues in between the users and this model also lacks security issues. In another model, named as DMTF – distributed management task force which enables the interoperability in multi-cloud environment. In reservoir model, which works with federated model of the cloud computing in this different cloud service providers came together to provide cloud services under one platform. Cloud foundry is framework which grants the power to the organisations or developers to distribute the workload on different servers by keeping the workload in mind. In this distributing the workload is only possible because in this system the applications by spiting the applications from its infrastructure.

Table 1: Model and its Aim

Model, Researcher/es	Aim
CHARM (Zhang et.al, 2015) [7]	Cost-efficient multi cloud data hosting mechanism where availability is the main priority. [6]
EGI Federated Cloud [8]	EGI Federated cloud integrates public, private or hybrid cloud in the form of multi-national cloud system. [6]
Distributed Management Task Force (DMTF) Architecture (Paper et al.,2009) [9]	Open Cloud standards Incubator models for enabling interoperability in multi-cloud environment. [6]
Reservoir Model (Rochwerger et al., 2009) [10]	Reservoir model for federated cloud computing. [6]
Cloud Foundry [11]	It aims to provide a standardized platform to the applications of customers by decoupling the application from its infrastructure. [6]

As we can see from the above paragraph and from table number 1 above and table number 2 below, we can see currently existing models and architectures lacks in maintaining the security and confidentiality of the data in multi-cloud environment. In table number 2, we will discuss about the following five models; CHARM, EGI Federated Cloud, Distributed Management Task Force, Reservoir Model, Cloud Foundry. Let us discuss about the above mentioned five models and architectures in table number 2.
Following is the table number 2: Strength & Weaknesses of various models and architectures.

Table 2: Strength & Weakness

Strength	Weakness
CHARM (Zhang et.al, 2015) [7]	
It distribute the data on multiple clouds in cost effective manner. [**6**]	Security is the main concern in this model. [**6**]
EGI FEDERATED CLOUD [8]	
User can access all services of cloud federation with a single identity. [**6**]	It lacks trust & unauthorized access issues and other security features not considered. [**6**]
DISTRIBUTED MANAGEMENT TASK FORCE (DMTF) ARCHITECTURE (Paper et al., 2009) [9]	
They have conceptually provided Incubator models for handling inter-operability in multi-cloud environment. [**6**]	Service Provider is unaware of this resource provisioning. So, lack of reliability and trust. Security is major concern that is not included here. [**6**]
RESERVOIR MODEL (Rochwerger et al., 2009) [10]	
The resource usage optimization at each reservoir site. [**6**]	Security, access feature, management of various multi-cloud architecture are not discussed. [**6**]
Cloud Foundry [11]	
The organizations can easily decide on where to deploy workloads. [**6**]	This model does not handle load balancing, security, and data issues. [**6**]

As we can analyse from the table 1 and table 2, we can conclude that over the span of time, several models and architectures which are proposed by various researchers, lacks in ensuring privacy and security of the data. As we can see further, Just as [**12**] there are threats on-premises environments, there are threats that affect multi-cloud environments too. Considering the diversity of threats that can affect an organization's cloud environment, it is no surprise that 73% of organizations are very or extremely concerned about cloud security. The above information is collected from the study conducted by Cisco in which we can see that threats and data breaches are a big concern for organisations as it poses risks to the privacy of the data. Botnets, malware, ransomware attacks are very common on cloud platforms. "Many traditional security solutions [**12**] still in use today just are not capable of adequately protecting increasingly dynamic and distributed multi-cloud strategies. As organizations navigate their path in the cloud, it is imperative that they leverage solutions that offer an integrated approach to security. In doing so, they can better prepare themselves to handle the complex cybersecurity challenges of today and the future," said Adwait Joshi, Director of Cloud Security product marketing at Microsoft.

"When considering [**13**] the challenges facing today's businesses, people and technology take centre stage. On one hand, companies need to bolster the workforce with well-trained security professionals who understand their roles and responsibilities. On the other hand, there is a pressing need for effective technology and tooling that both addresses the rapidly evolving landscape of cybersecurity threats while effectively supporting security teams," said Hillary Baron, lead author and Senior Technical Director for Research, Cloud Security Alliance. "It's clear that today's multi-cloud environments are increasingly complex, and enterprises must find ways to comprehensively address their security posture." It is clear from the above that relevant parties and groups are plagued by a serious problem of data privacy and security. The cloud industry needs a unique and robust system which can ensure security of the data.

As researcher [**14**] emphasized the importance of use of the intrusion detection system to ensure the security of the data. It will help in tackling with the cyber threats and data breaches from the malicious entities. Intrusion detection system further categorized into two categories namely, HIDS and NIDS. HIDS refers to host-based intrusion detection system and NIDS refers to network-based intrusion detection system.

Host based intrusion detection system (figure 1) is a program installed on the host systems to detect and mitigate the cyber-attacks. It uses the agents that continuously monitors the host system like personal computers, servers, or any other computing device. It continuously monitors the network traffic for that particular host and it actively monitoring any changes in the configuration files, system file modifications. HIDS works on the basis on two principles, signature-based detection, and anomaly-based detection.

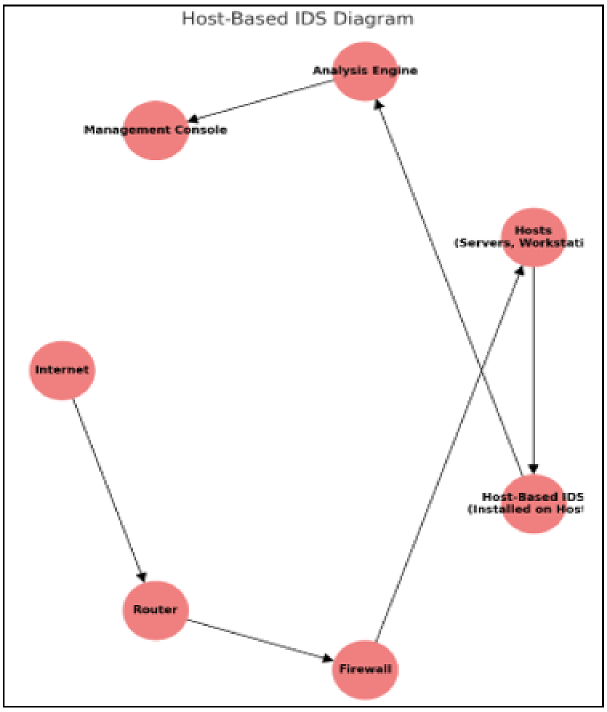

Figure 1: Host IDS (HIDS)

Network based intrusion detection system (figure 2) is deployed on the network of the organisation. NIDS continuously monitor the network on which it is installed on. NIDS works on passive mode; it alerts the users of any suspicious activity. It also based on two principles anomaly-based detection and signature-based detection. NIDS actively monitors the incoming and outgoing traffic in order to detect the intrusions and sends the alerts to appropriate entities to take further actions.

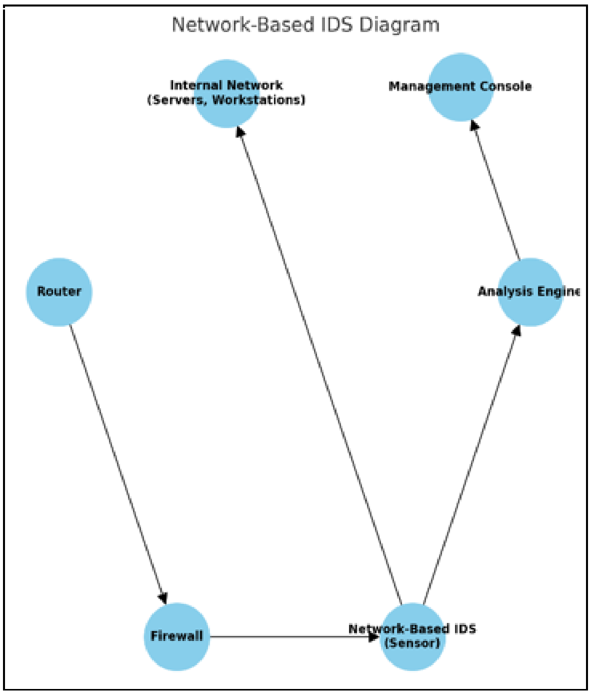

Figure 2: Network IDS (NIDS)

3. Research Objectives

The objectives of our proposed research of automated data deletion system for multi-cloud environments extends across several key aspects. Following, are some of the key aspects of research significance:

3.1 It will enhance the data security and mitigate the threats by automatically deleting sensitive data upon detecting intrusions.

3.2 The proposed research will employ the Zero Trust Security Model. ZTS model is highly popular in the field of cloud computing and cyber security, in this no user or system is trusted, thus ensuring security of data.

3.3 The proposed research design directly aligns with the compliance regulations which ensures the protection of the data by stringent data protection rules and regulations such as GDPR, CCPA, HIPAA, DPDPA.

3.4 The proposed system will implement the logging of all the activities and implementation of auditing capabilities; it will ensure the proper management of the system.

3.5 Implementation of automation in our system will ensure the minimization of the human made errors. In this, data will automatically delete as soon as intrusion is detected, thus enhances overall efficiency of the system.

3.6 This research will offer a practical solution to the organisations who deals with highly sensitive and confidential data.

3.7 This research will provide a blueprint to the stakeholders to establish, design and implement the data security measures.

3.8 This research will further lay a foundation for the future studies related to the data security and protection.

4. Proposed Work

In this research, we aim to develop an automated system for the security of the data. This system will mitigate the data threats and protect the system from data breaches. The system will also adhere to regulatory compliance such as GDPR, CCPA, HIPAA, and DPDPA. We planned to include the following modules in our proposed system (figure 3), policy module, data deletion module, intrusion detection module, cloud APIs module, logging and monitoring module, and reporting and dashboarding module. Let us discuss the above modules in brief; Policy module, which handles all the working of the automated system. In this the stakeholders will establish the policies related to data deletion and regulatory compliance. Data Deletion module will handle the deletion of the data as soon as intrusion is detected. Intrusion Detection System module actively monitor the network to detect any data breach into the system. Cloud APIs module will be used to communicate with multi-cloud platforms. It enables two components to interact together using different set of policies and protocols. Logging and Monitoring module maintains all the logs like system logs, intrusion detection logs, and compliance logs and monitoring part of the module will actively monitor the automated data deletion system and network which it is going to be installed on. Reporting and Dashboarding module will provide a graphical user interface to the stakeholders and gives insight to system metrics. In this stakeholder can get the insight to system performance and information about data deletion activities and intrusion detection activities. Through this research, the goal is to subsidize the improvement in data management practices in multi-cloud environments and provide the relevant groups with effective tools and methodologies for ensuring data privacy and security in the multi-cloud.

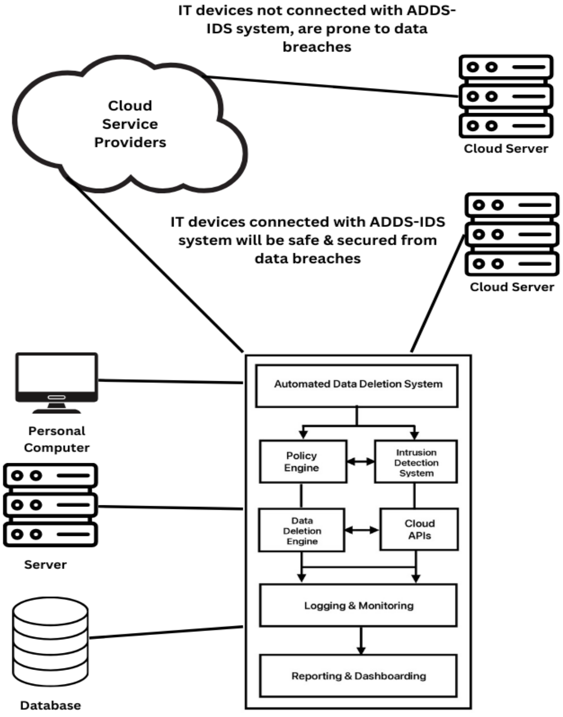
IT devices not connected with ADDS-IDS system, are prone to data breaches
Cloud Service Providers
Cloud Server
IT devices connected with ADDS-IDS system will be safe & secured from data breaches
Cloud Server
Personal Computer
Server
Database
Automated Data Deletion System
Policy Engine
Intrusion Detection System
Data Deletion Engine
Cloud APIs
Logging & Monitoring
Reporting & Dashboarding

Figure 3: Proposed System and its working

5. Conclusion

In this research, the system is proposed which will ensure the security of the data over multi-cloud platforms. It will protect the data from data breaches and mitigate the threats. In this proposed system, data will be automatically deleted as soon as intrusion is detected. This research will increase the confidence in users that their data is well protected in multi-cloud environment. This system is going to encourage the stakeholders to use cloud services instead of traditional systems to store and manage the data. The usage of zero trust model architecture in our system, increases the confidence in the users that their data is well protected and secured. This research will provide a blueprint to the stakeholders to establish, design and implement the data security measures. It will also offer a practical solution to the organisations who deals with highly sensitive and confidential data and maintains high-level security. Further, we are trying to implement this proposed system in real-world scenario.

References

[1] Dr. Blesson Varghese, Dr. Rajkumar Buyya Next generation cloud computing: New trends and research directions. DOI: 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. (2022). 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. https://doi.org/10.1007/978-3-030-74402-1_15

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

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

[6] 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

[7] 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

[8] 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

[9] I. Clouds, “A white paper from the open cloud standards incubator,” Distributed Management Task Force, Version, vol. 1, 2009.

[10] 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.

[11] 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

[12] Multi-cloud security: architecture and ultimate guide https://www.cisco.com/site/in/en

[13] Cloud Security Alliance Survey Finds Complexity of Multi-cloud Environments Driving Use of Cloud Native Application Protection Platforms, 2023 https://cloudsecurityalliance.org/

[14] Suman Lata, Dheerendra Singh, Intrusion detection system in cloud environment: Literature survey & future research directions, International Journal of Information Management Data Insights, Volume 2, Issue 2, 2022, 100134, ISSN 2667-0968, https://doi.org/10.1016/j.jjimei.2022.100134

Author 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 rindustry 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**.