**MODEL FOR SECURED DATA STORAGE ON PUBLIC CLOUD**

**Dr.K.Dhanalakshmi\*1 ,Hemaroshini M\*2, Janani R\*3, Kaviya M\*4, Malavika A C\*5**

\*1Professor, Department of CSE, PSNA CET, Dindigul, TamilNadu, India

\*2,3,4,5Students, Department of CSE, PSNA CET, Dindigul, TamilNadu, India

**ABSTRACT**

The main aim of the project is to create a model for secured data storage on public cloud. The use of online services is expanding daily, having a significant impact on businesses switching to cloud-based services. The main concern in cloud is the amount of storage required and when scaled is it going to cut the budget that the corporation/organization must spend. The proposed system works on multi data storage using secret key sharing algorithm. The user can upload their files on the cloud and the file is split into three parts by secret sharing algorithm. The necessary blocks are encrypted by Advanced Encryption Standard (AES) algorithm. This provides high security to the data stored on the cloud. The user can retrieve the decrypted data by requesting the domain manager for a dynamic secret key and storage protection scheme for addressing access control. In our model, all the cryptographic operations are performed on trusted IaaS compute hosts and storage protection scheme for addressing access control. This provides high security to the data stored on the cloud. This uses the cloud services more efficiently and effectively with very low downtime.

**Keywords:** Public Cloud, Dynamic Secret key, Random Split, Encryption, Decryption, Secret Key Sharing

1. **INTRODUCTION**

The rapid adoption of cloud computing has been accompanied by an increasing demand for secure data storage solutions. Threats and mitigation techniques for the IaaS model have been under intensive scrutiny in recent years while the industry has invested in enhanced security solutions and issued best practice recommendations. Despite the inherent convenience of public clouds, organizations reluctance to store critical data on public cloud platforms is primarily due to concerns around privacy, confidentiality, and data breaches. To address these concerns, we propose a model for secured data storage on public cloud platforms. The proposed model employs a combination of encryption and access control mechanisms to protect sensitive data assets. The model provides key features such as data encryption, authorized access, and auditability, which help in ensuring the security of the data stored on the public cloud. Additionally, the model is based on a multi-level security framework that segregates data based on its sensitivity and importance, thus providing an added layer of security to the data. Through this model, we aim to build a secured, reliable solution for all organizations seeking to store and manage their data on public cloud platforms while ensuring that they can trust and depend on their chosen cloud service provider.

1. **PROBLEM STATEMENT**

In recent years, cloud computing has emerged as an efficient way for individuals and organizations to store, process, and access data on the internet. Public cloud environment offers several advantages such as scalability, cost effectiveness, and accessibility. However, the shared responsibility model of cloud security means that the cloud service provider is only responsible for the security of the cloud infrastructure, leaving the responsibility of securing the data on the customer and particularly in public clouds where data is shared with multiple users. With the increasing reliance on public cloud services, it is becoming the critical to develop effective solutions for secure data storage on public clouds. Therefore, the challenge is to develop a model for secure data storage on public cloud that ensures the confidentiality, integrity, and availability of data, while also complying with regulatory and compliance requirements. The model must be able to protect data from unauthorized access, data breaches, and loss while maintaining the usability and accessibility of the data. It should consider the performance and cost implications of implementing security measures on the cloud infrastructure.

1. **EXISTING SYSTEM**

The current model for secured data storage on public clouds allows for the establishment of trust by remotely attesting host platform configuration prior to the launch of guest virtual machines and ensures data confidentiality in remote storage with encryption keys maintained outside of the IaaS domain. The legitimacy and effectiveness of the suggested protocols are shown by the experimental data presented [3]. The framework prototype was put into use on a test platform running a public electronic health record system, demonstrating the viability of integrating the suggested protocols into current cloud environments. These public cloud service companies provide customers with monitoring and logging services that let them examine how their data is being used. This can aid in the detection and prevention of security concerns as well as assist clients in making the best use of the public cloud [2]. To guarantee that data is safeguarded from security threats and complies with regulatory standards, public cloud providers offer a variety of security and compliance safeguards.

1. **DRAWBACKS OF EXISTING SYSTEM**
* Security Risks: Storing sensitive data on a public cloud can create potential security risks, as it involves sharing infrastructure and resources with other users, making it more susceptible to cyberattacks and data breaches.
* Cost Implications: The cost of storing data on public clouds can quickly add up, especially for businesses with large amounts of data. This can create financial constraints and make it difficult to scale as the business grows.
* Compliance Challenges: Public cloud storage models may not always comply with certain data protection regulations, making it difficult to ensure data privacy and security.
* Performance and Availability: Public cloud services are subject to outages and can experience performance issues due to high demand or technical problems. These issues can affect the availability and accessibility of data stored on the public cloud.
1. **PROPOSED SYSTEM**

The proposed system is more efficient and secure which removes all the drawbacks of the existing system. It presents an Infrastructure as a service (IaaS) storage protection scheme addressing access control. The authors analyze access rights management of shared versioned encrypted data on cloud infrastructure for a restricted group and propose a scalable and flexible key management scheme. Access rights are represented as a graph, making a distinction between data encryption keys and encrypted updates on the keys and enabling flexible join/leave client operations. Despite its advantages, the requirement for client-side encryption limits the applicability of the scheme and introduces important functional limitations on indexing and search.

1. **FEASIBILITY STUDY**

Preliminary investigation examines project feasibility, the likelihood the system will be useful to the organization. The main objective of the feasibility study is to test the Technical, Operational and Economical feasibility for adding new modules and debugging old running systems. All systems are feasible if they have unlimited resources and infinite time. There are aspects in the feasibility study portion of the preliminary investigation:

* Technical Feasibility
* Operational Feasibility
* Economical Feasibility

 **6.1 TECHNICAL FEASIBILITY**

The technical issue usually raised during the feasibility stage of the investigation includes the following:

* Does the necessary technology exist to do what is suggested?
* Does the proposed equipment have the technical capacity to hold the data required to use the new system?
* Will the proposed system provide adequate response to inquiries, regardless of the number or location of users?
* Can the system be upgraded if developed?
* Are there technical guarantees of accuracy, reliability, ease of access and data security?

Earlier no system existed to cater to the needs of ‘Secure Infrastructure Implementation

**6.2** **OPERATIONAL FEASIBILITY**

Proposed projects are beneficial only if they can be turned out into an information system. That will meet the organization’s operating requirements. Operational feasibility aspects of the project are to be taken as an important part of the project implementation. Some of the important issues raised are to test the operational feasibility of a project includes the following:

* Is there sufficient support for the management from the users?
* Will the system be used and work properly if it is being developed and implemented?
* Will there be any resistance from the user that will undermine the possible application benefits?

This system is targeted to be in accordance with the above-mentioned issues. Beforehand, the management issues and user requirements have been taken into consideration. So there is no question of resistance from the users that can undermine the possible application benefits. The well-planned design would ensure the optimal utilization of the computer resources and would help in the improvement of performance status.

**6.3** **ECONOMICAL FEASIBILITY**

A system can be developed technically and that will be used if installed must still be a good investment for the organization. In the economical feasibility, the development cost in creating the system is evaluated against the ultimate benefit derived from the new systems. Financial benefits must equal or exceed the costs. The system is economically feasible. It does not require any additional hardware or software. Since the interface for this system is developed using the existing resources and technologies available at NIC, There is nominal expenditure and economical feasibility for certain.

1. **METHODOLOGY**

**7.1 User Module**

Self registration forms are used to create a new account with the system. It requires the user to enter their personal information. After the user has filled out the form, they will be able to log in to the system. The system checks the user credentials and if the credentials are correct, a request is sent to the system. Admin sends a dynamic secret key(OTP) and this ensures that only the user with access to the email account can upload files into the cloud storage. It also prevents unauthorized access to the cloud storage. The uploaded files are randomly splitted into three parts, encrypted using a secure encryption algorithm, and stored in the cloud server. The splitting of the files is implemented using a secret sharing algorithm. Secret sharing is a cryptographic techniques for dividing a secret into many shares and giving each share to a different party. A breacher who obtains fewer shares of the secret than the threshold does not learn anything about the secret. The Advanced Encryption Standard(AES) algorithm is used to encrypt and decrypt the blocks. The TPA verifies the files after they have been uploaded. The user can choose whether to allow or deny each request by viewing them all on the alerts tab for a particular file. Hence, without the user's consent, a third party cannot access the files.

**7.2 Admin Module**

The administration is provided with separate admin credentials. All of the details regarding the files that users have uploaded are visible to the administrator. The admin has access to the data that the user gave during registration. The admin can view the user's activity on the website. They can also view the files that the cloud user has uploaded, along with any associated information. The admin can also delete any user accounts or files that are deemed inappropriate or offensive. When a user rejects the TPA’s request to access the file and verify the contents, the admin considers the file as a malicious content and delete it from the cloud. They also ensure that the cloud environment is secure and compliant with industry standards and regulations. Admin is responsible for managing and maintaining the cloud users.

**7.3 Third Party Auditor Module**

TPA is an expertise authorized client and used for auditing purpose. TPA’s are typically hired by cloud customers to audit their cloud provider's security practices and ensure compliance with their standards and regulations. TPA request the user for permission to access the file. If the user grants permission, the TPA may access and download the file. TPA examines the files that the user has uploaded. TPA has the ability to request access for a certain file from the user. The user chooses whether to approve or reject the request. When the user responds and chooses to accept, the TPA can examine the response and download the file. TPA’s are typically hired by cloud customers to audit their cloud provider's security practices and ensure compliance with their standards and regulations. TPA examines the file that users have uploaded. TPA’s assist in ensuring that cloud service providers uphold their duties to their clients in terms of security. Customers can also get assurance from TPAs that their data is processed and kept securely in the cloud. Each entity obtains a certificate via a trusted certification authority.

**7.4 Cloud Service Provider Module**

CSP is responsible for managing and maintaining cloud computing systems. When a user uploads a file on cloud, cloud service provider distributes a file into different servers. The cloud administrator maintains the functionality of cloud infrastructure, assisting in cloud service deployments and working alongside other cloud roles to ensure the network functions well. Access to the cloud is only permitted for authenticated users. It is responsible for managing and maintaining cloud computing systems. This includes setting up, configuring, and monitoring cloud-based applications and services. Cloud manages the website's settings. The cloud administrator maintains the functionality of cloud infrastructure, assisting in cloud service deployments and working alongside other cloud roles to ensure the network functions well. The cloud administrators must select and operate tools for cloud storage management, [high availability](https://cloud.netapp.com/blog/understanding-aws-high-availability-compute-sql-and-storage), [cloud migration](https://cloud.netapp.com/blog/cloud-migration-strategy-challenges-and-steps) and [optimization of cloud cost](https://spot.io/resources/cloud-cost/cloud-cost-optimization-15-ways-to-optimize-your-cloud/)s.

1. **SYSTEM ARCHITECTURE**

****

**Figure 1:** System architecture diagram

Figure 1 represents the system architecture. The user uploads the file in the cloud by requesting a dynamic secret key from admin and therefore unauthorized access are restricted. The uploaded files are randomly splitted into three parts, encrypted using a secure encryption algorithm, and stored in the cloud server. The splitting of the files is implemented using a secret sharing algorithm. The uploaded files are verified by the TPA. The TPA request access for the file to the user to verify the contents of the file. If the user grants access, the TPA downloads the file and verifies the content. If the user rejects the request, the admin treats the file as a malicious content and removes the file from the cloud so only authorized contents are stored in the cloud.

1. **RESULTS AND DISCUSSION**
	1. **Splitting and encryption of blocks**

A user-uploaded file is arbitrarily divided into three blocks, and each block is encrypted in accordance with the user's requirements. The choice to encrypt or not to encrypt a given block is made by the user.

****

**Figure 2:** Splitting and Encryption on Blocks

* 1. **File verification by TPA**

The contents of the file uploaded by the user is verified by the TPA. The TPA requests user for access to the file. If the user agrees to the request, the TPA can obtain the file that has been decrypted and check its contents. The admin considers the file as malicious content and deletes it from the cloud if the user rejects the request.

****

**Figure 3 :** File verification by TPA

.

1. **CONCLUSION**

The model of secured data storage on the public cloud provides a secure and reliable way to store data on the cloud. It ensures that the data is encrypted and stored in a secure environment, and that access to the data is restricted to authorized users. By implementing the proposed model, organizations can optimize their cloud storage resources and reduce storage costs, while also improving data access and retrieval times. In this work we presented a framework for trusted infrastructure cloud deployment, with two focus points: VM deployment on trusted hosts and domain-based protection of stored data. We described in detail the design, implementation and security evaluation of protocols for trusted VM launch and domain-based storage protection. Furthermore, the model's scalability and flexibility make it well-suited for a variety of industries and applications. As cloud adoption continues to grow, the need for efficient data storage solutions will become increasingly important, and the model presented here can serve as a valuable tool for organizations seeking to improve their cloud storage capabilities.

1. **REFERENCES**
2. Rafique, A.; Van Landuyt, D.; Beni, E.H.; Lagaisse , B.; Joosen, W. CryptDICE: Distributed data protection system for secure cloud data storage and computation. Inf. Syst. 2021, 96, 101671
3. Venkatesan, B.; Chitra, S. An enhance the data security performance using an optimal cloud network security for big data cloud framework. Int. J. Commun. Syst. 2021, e4854.
4. Rashmi, P.; Supriya, M.C.; Hua, Q. Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare. Secure. Communication Netw. 2022, 2022, 9363377.
5. Zhou, Z.; Zhao, L. Cloud computing model for big data processing and performance optimization of multimedia communication. Computer. Communication. 2020, 160, 326–332.
6. Ming, Y.; He, B.; Wang, C. Efficient revocable multi-authority attribute-based encryption for cloud storage. IEEE Access 2021, 9,42593–42603
7. Yinbin Miao.;Robert H. Deng.; Kim-Kwang Raymond Choo.; Ximeng Liu.; Hongwei Li.Threshold Multi-keyword Search for Cloud-Based Group Data Sharing.2020.
8. Qinlong Huang.; Yixian Yang.; Wei Yue.; Yue He.Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing.2019
9. Xuyang Wang.; Aiqun Hu.; Hao Fang.Multi-User File-Sharing Systems Based on LWE.2020
10. Yunjun Zheng.; Weiwei Xia.; Long Jiang.; Feng Yan.; Lianfeng Shen.Distributed Multi-agent Cooperative Resource Sharing Algorithm in Fog Networks.2020.
11. Jiang Du.; Junhai Zhou.; Yaping Lin.;Wei Zhang.; Jianhao Wei.Secure and Verifiable Keyword Search in Multiple Clouds.2021.