ENHANCING MULTI-CLOUD SECURITY USING SHAMIR'S SECRET SHARING ALGORITHM

Moram Sunil Kumar Reddy[1] , Dr. Manoj Eknath Patil[2]

[1] Research Scholar, Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh.

[2] Supervisor, Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh.

ABSTRACT

Shamir's Secret Sharing is a cryptographic technique for secret distribution that guarantees a secret can only be reconstructed with a certain minimum number of pieces. Protecting sensitive information against unauthorized access and reducing the risks of data breaches may be achieved using this threshold-based strategy. This article discusses potential solutions and methods, as well as an overview of many ongoing research papers, all pertaining to the security of single and multi-cloud environments utilizing Shamir's Secret Sharing algorithm. The primary goal of this work is to decrease security threats and their impact on cloud computing users via the use of Shamir's Secret sharing technique in conjunction with multi-cloud data protection. It is a method of sharing secrets in which a secret is broken down into smaller pieces and given to each participant; in order to reassemble the secret, it may be necessary to use some or all of the pieces.

Keywords: *Secret Sharing, Data integrity, Cloud, Intrusion, Service.*

I. INTRODUCTION

Data protection in dispersed cloud systems has taken a giant leap forward with the implementation of Shamir's Secret Sharing Algorithm, which improves multi-cloud security. Due to the distributed nature of their data, enterprises face substantial security concerns when they embrace multi-cloud strategies to use different cloud service providers' capabilities. Data storage and processing in multi-cloud systems need strong safeguards to protect the privacy, authenticity, and accessibility of critical data. Due to their ineffective risk management of data fragmentation and breaches, traditional security systems often fail to meet these demands.

An advanced method to address these security issues was proposed by Adi Shamir and named Shamir's Secret Sharing Algorithm. To implement this cryptographic method, several cloud providers are each given a portion of a secret, called a share. So that no one party has full knowledge, the initial secret must have a certain minimum number of shares in order to be rebuilt. By spreading the workload around, this method greatly improves security by making data leakage less likely. Even if an attacker manages to breach more than one cloud provider, they will only be able to decipher a small portion of the secret, leaving them unable to recreate all of the sensitive data.

When businesses use Shamir's Secret Sharing Algorithm, they may protect their multi-cloud installations from several dangers, such as hackers and data breaches. This algorithm ensures that sensitive information is secured across different platforms, which not only increases data security but also helps with compliance with legal obligations. In order to tackle the rising security concerns and safeguard important company data, it is crucial to include sophisticated cryptographic methods such as Shamir's Secret Sharing into multi-cloud tactics.

A significant step forward in protecting data across various cloud settings has been made possible by improving multi-cloud security utilizing Shamir's Secret Sharing Algorithm. To maximize performance, provide redundancy, and lessen the chances of vendor lock-in in this age of cloud computing, multi-cloud methods are being used more and more by companies. Nevertheless, safeguarding sensitive data's privacy and integrity becomes more difficult in multi-cloud systems due to their dispersed nature. To overcome these difficulties, Adi Shamir devised the cryptographic method known as Shamir's Secret Sharing Algorithm. This method involves splitting a secret into many pieces, or shares, and then distributing them across several cloud providers. Reconstructing the original secret only requires a preset subset of these shares, which enhances security. This method lessens the likelihood of data breaches and illegal access by making sure that no one cloud provider has full knowledge of the secret. Organizations may enhance their defenses against internal and external attacks by incorporating Shamir's Secret Sharing Algorithm into multi-cloud security frameworks. In addition to bolstering data security, this approach helps in meeting demanding regulatory standards. With the constantly-changing landscape of multi-cloud settings, it is more important than ever to handle new security problems and protect vital company data by using modern cryptographic approaches such as Shamir's Secret Sharing.

II. REVIEW OF LITERATURE

Chhabra, Sakshi & Singh, Ashutosh. (2020). With the advent of cloud computing, the IT sector has finally realized some of its long-sought goals, like the provision of distant storage services and privacy solutions. It is a paradigm for storing data that allows for its management, preservation, and presentation to users across a network. Nevertheless, there are security considerations associated with cloud storage. Maintaining group confidentiality is one of the primary areas of cloud storage study. One of the most prominent approaches of protecting sensitive information is the Secure Secret Sharing (SSS) mechanism, which is the subject of this article. Only qualified participants (Qn) are provided portions of the produced secret key, and the suggested approach uses the index buffer and malicious checkers to assess it before sharing encrypted data over the cloud. Whether individuals demonstrate themselves to be allowed participants or not, this malicious checker uses their past performances to verify them. An independent entity known as a key handler (KH) stores the key share; KH is an integrated method for handling, reconstructing, and decrypting key shares. Cloud providers will divulge sensitive information to their owners if the Key Handler (KH) obtains more than 80% of the secret key; however, if KH obtains 90% of the key, cloud providers will divulge just one top secret. Reconstructing the secret from shares is accomplished using Lagrange's interpolation approach. In our experiment, the writers have taken into account two standards for testing and analyzing the outcomes. To demonstrate the effectiveness of our method, we measure its performance using time consumption and probability computation. A total of 1176.35 milliseconds were required for processing, and 96.1265 milliseconds were used to generate keys for 128 shares by over 100 customers. Our approach enhances security and decreases risks by 43.82 percent across all analyses for safe cloud data exchange.

Althamary, Ibrahim & Alkharobi, Talal. (2016). Cloud computing is a major paradigm for enabling networked, on-demand access to shared resources, including data, software, infrastructure, and platforms. Availability, secrecy, and integrity are three things that cloud storage must have. Users are encouraged to use a highly secure protocol due to the sensitivity and worth of the information. In this paper, we provide a novel approach to secret sharing as a means to enhance user confidence in cloud computing. Any file format may be converted to ASCII strings utilizing the suggested algorithm's use of Base64 encoding. In order to speed up the process of constructing shares, Base64 strings do not need any further compression. Using the Shamir Secret Sharing Scheme, we can generate N shares from each string, and then we can store each share in our own cloud storage space.

AlZain, Mohammed et al., (2015) Businesses may take advantage of on-demand, cost-effective data management using cloud computing, a remarkable distributed computing paradigm. Concerns about the privacy and security of company data arise from this so-called outsourcing of computer resources. Unfortunately, none of the solutions that have been suggested so far address multi-clouds in any way. A data management paradigm for both public and private multi-cloud environments is presented in this study. The suggested paradigm, BFT-MCDB, enhances the reliability and safety of company data storage via the use of Shamir's Secret Sharing method and the Quantum Byzantine Agreement protocol, all while maintaining performance. The assessment of performance is done using CloudSim, a cloud computing simulator. Results from experiments demonstrate that this model outperforms other popular cloud cryptography based methods in terms of both data storage and data retrieval. The suggested strategy for managing data across several clouds is feasible, according to the results of the performance study conducted using CloudSim.

Muhil, M. et al., (2015) An up-and-coming technology, cloud computing is now dominating the information technology sector. Data storage, retrieval, and processing on the cloud are state-of-the-art technologies used globally. You may choose from a variety of service models and deployment strategies using cloud computing. These capabilities make it easier to outsource data storage to third-party services. The supplier of storage must guarantee the security of the user's data, allow queries on the data, and ensure that the provider cannot see the results of such queries. For the purpose of data outsourcing security, methods such as data encryption, homomorphic encryption, and secret sharing algorithms are often used. Problems with CIA (Confidentiality, Integrity, and Availability) are the most common in data storage management. Users and consumers are increasingly choosing "multi-cloud" or "cloud of clouds" or "interclouds" solutions since single clouds have several security flaws. Secret Sharing Algorithms are one of the methods used to protect these multi-clouds. A wide variety of secret sharing algorithms are available. This article discusses how to protect data outsourcing in a multi-cloud environment using Shamir's secret sharing method.

Alam, Md & Kather, Sharmila. (2013). Many organizations and IT sectors are quickly adopting cloud computing because it offers new software at cheap cost and has a strong growth rate [1]. As a result, cloud computing provides us with a plethora of advantages, including accessibility to data over the Internet and affordable costs. The primary consideration in a cloud computing environment is the assurance of security threats associated with cloud computing. For instance, users may entrust cloud storage providers with sensitive information. The hazards of service availability failure and the possibility of malevolent insiders in a "single cloud" make it less attractive with consumers. Currently, a trend toward "multi clouds," "multiple clouds," or "cloud-of-clouds" is being seen via the implementation of Shamir's Secret Sharing Algorithm. This article examines many ongoing studies that deal with the security of single and multi-cloud environments via the use of Shamir's Secret Sharing algorithm, and it discusses potential solutions and methodologies in this area. The primary objective of this work is to decrease security threats and their impact on cloud computing users via the use of multi-cloud computing and the Shamir's secret sharing technique. This method of secret sharing involves breaking a secret into smaller pieces and giving each participant a unique piece. In order to piece together the secret, either all of the pieces must be found or at least some of them must be known. Since it can be impossible to count all participants in order to combine the secret, the threshold approach is employed in cases where any "k" of the parts can be utilized to reconstruct the original secret.

B.Arun et al., (2012) Computing in the cloud refers to a set of services that enable users to access and store data and compute without requiring them to have any specific technical expertise. Many businesses have recently begun to rely on cloud computing. A lot of large companies have already made the switch to cloud computing and are using it to their advantage with smart working, remote services,

and security. Although there is no one-size-fits-all reason for using cloud computing, the most common ones are financial, operational, and security-related. As a result of the dangers of service availability failure and malevolent insiders in a single cloud, "single cloud" companies are expected to lose popularity among consumers. The academic community has largely ignored the usage of multi-cloud providers to ensure security in favor of single clouds. Because of its potential to lessen security threats that impact cloud computing users, this effort seeks to encourage the usage of multi-clouds.

III. RESEARCH METHODOLOGY

Customers of cloud services might build their expectations according to their prior encounters and the requirements of their companies. Prior to selecting a cloud service provider, they will probably do a survey. Additionally, customers are required to conduct security tests based on the three tenets of security: availability, confidentiality, and integrity. Conversely, cloud service providers may make grand claims to win over customers, but unfulfilled promises might become insurmountable roadblocks down the road. This is something that many prospective cloud clients are aware of, yet they are still likely to take a back seat. Without assurance that all gaps are manageable, they will not go further with cloud computing. In Figure.1, all the important details about cloud computing security are shown in a single image. There are three parts to our cloud computing security framework: classifications of security, models of security in service delivery, and dimensions of security.

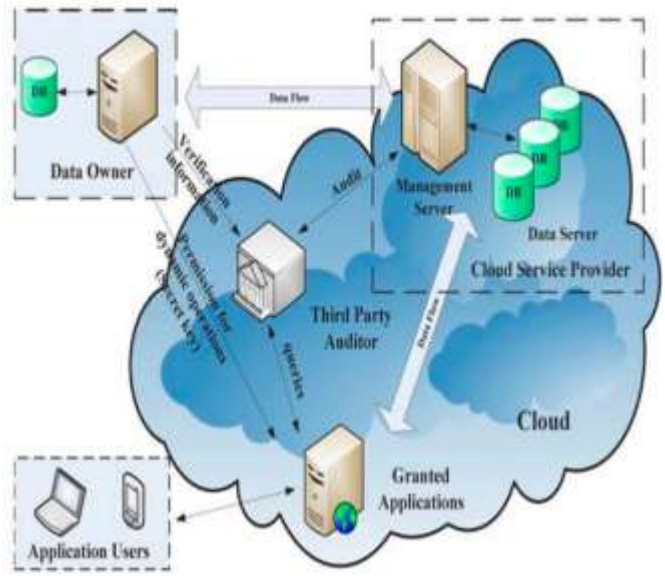

Figure 1: Cloud Computing Security

Algorithm Used

Shamir's Enigma Distributing Programs the security of data kept in the cloud is not guaranteed. Therefore, we need to devise a strategy to protect such data. To address concerns about disclosure, we may encrypt them before uploading them to the cloud.

The ability to monitor their surroundings and relay findings to customers is a boon to service providers.

To avoid reports that mix events pertaining to distinct service customers, logs must be properly designed

to evaluate the actions of system administrators and other restricted users. Companies looking to use cloud solutions and those offering such solutions both have a responsibility to solve cloud security. Data protection, availability, compliance, privacy, Identity and Access Management (IAM), business continuity, disaster recovery strategies, and sound governance are just a few of the ways to keep your cloud secure. A snapshot of the aforementioned security measures is shown in the picture (picture 2) below.

Figure 2: Measures to ensure Security in Cloud.

IV. RESULTS AND DISCUSSIONS

Data Integrity

Data security is a major concern in the cloud because of the wide variety of client applications that depend on it. Since the client does not have a copy of all stored data, cloud computing for data maintenance may not be completely reliable. On the other hand, writers never inform us about data integrity by way of its user. To ensure data integrity both before and after cloud insertion, we must develop a new system based on our data reading protocol algorithm. Here, the client verifies the data's security both before and after with the aid of the CSP by utilizing our "effective automatic data reading protocol from user as well as cloud level into the cloud" in an honest manner.

Data Intrusion

The significance of cloud computing's data intrusion detection systems. We learn about the various host, network, and hypervisor-based intrusion detection choices, as well as how software as a service, platform as a service, and infrastructure as a service offers handle intrusion detection. The reality we live in includes attacks on data and systems. As far as security measures are concerned, it is now

considered due care to detect and react to such assaults.

Service Availability

One of the most crucial aspects of cloud computing security is the availability of services. The possibility of service outages is something that Amazon acknowledges in its license agreement. Any files uploaded by the user that violate the cloud storage policy will result in the immediate and permanent termination of their web service. Furthermore, the Amazon Company will not be held financially responsible in the event that any of its online services are damaged and subsequently fail. Businesses who want to safeguard their services from this kind of disaster can implement steps like using several providers or creating backups.

DepSky System Model Architecture

Readers and writers are client-side responsibilities inside the DepSky system concept, which also includes four cloud storage providers. Cloud storage readers and writers are defined differently by Bessani et al. Writers can only fail by crashing, but readers may fail for any reason (e.g., they can crash sometimes and then act whatever they choose). Figure 3 shows the four cloud configuration in the DepSky model.

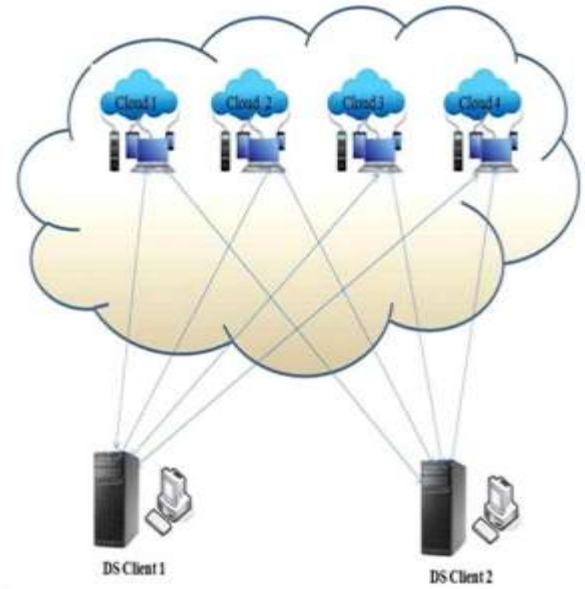

Figure 3: DepSky Architecture

Preliminary, initiation, and closing activities are the three main phases that make up the scope of any cloud computing system. The preparatory tasks cover a lot of ground, from figuring out what the company needs in terms of privacy and security to assessing the security provider's offerings and the risks associated with meeting the organization's control goals.Vukolic proposed using dependable distributed storage in multi clouds or interludes that use a subset of Byzantine fault tolerance (BFT) approaches. The HAIL (High Availability and Integrity Layer) protocol is one example of a system that handles many clouds.With HAIL, a customer can be certain that their data is both accessible and intact across all of their cloud storage locations, and the service also offers a software layer to handle issues with data availability and integrity.

V. CONCLUSION

Finally, one of the best ways to deal with the complicated security issues that arise in dispersed cloud systems is to improve multi-cloud security by using Shamir's Secret Sharing Algorithm. Organizations may greatly improve the security of their critical data across several cloud platforms by using this powerful encryption approach. By dividing the secret into many shares and distributing them among several cloud providers, Shamir's Secret Sharing Algorithm reduces the likelihood of data breaches and illegal access. This method lessens the effect of security flaws by making sure no one supplier has enough data to deduce the whole secret. On top of that, this approach improves data integrity generally and is in line with regulatory standards. Integrating Shamir's Secret Sharing to protect vital company data will become more important as multi-cloud systems are used more widely. Organizations may strengthen their defenses against new threats and increase confidence in their cloud-based operations by employing strong security measures. In the ever-changing world of multi-cloud computing, Shamir's Secret Sharing Algorithm provides a useful tool for increasing security and resilience.

REFERENCES: -

[1] S. Chhabra and A. Singh, "Security Enhancement in Cloud Environment using Secure Secret Key Sharing," Journal of Communications Software and Systems, vol. 16, no. 4, pp. 1-9, 2020,

[2] Althamary and T. Alkharobi, "Secure File Sharing in Multi-clouds using Shamir's Secret Sharing Scheme," Transactions on Network and Communications, vol. 4, no. 6, pp. 1-7, 2016,

[3] M. AlZain, A. Li, B. Soh, and E. Pardede, "Multi-Cloud Data Management using Shamir's Secret Sharing and Quantum Byzantine Agreement Schemes," International Journal of Cloud Applications and Computing, vol. 5, no. 3, pp. 35-52, 2015.

[4] M. Muhil, U. Krishna, R. Kumar, and M. Anita, "Securing Multi-cloud Using Secret Sharing Algorithm," Procedia Computer Science, vol. 50, no. 1, pp. 421-426, 2015, doi: 10.1016/j.procs.2015.04.011.

[5] S. S. Mirajkar, S. Biradar, and C. Cachin, "Secret Sharing Based Approach to Enhance Security in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 6, pp. 53-57, June 2014.

[6] K. Sai Sowmya and M. Krishna Siva Prasad, "Efficient and Secure Auditing To Cloud Storage in Cloud Computing," International Journal of Computer Trends and Technology (IJCTT), vol. 16, no. 3, pp. 1-7, 2014.

[7] S. Gaidhankar, A. Kanase, T. Lonkar, and C. Patil, "Multi-Cloud Storage Using Shamir's Secret Sharing Algorithm," International Journal of Advancement in Engineering Technology Management & Applied Science, vol. 1, no. 7, pp. 1-7, December 2014.

[8] M. Alam and S. Kather, "An Approach to Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds," International Journal of Scientific and Research Publications, vol. 3, no. 4, pp. 1-8, 2013.

[9] "Review of Methods for Secret Sharing in Cloud Computing," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 1, pp. 1-8, January 2013.

[10] M. Kausar Alam and S. Banu K., "An Approach to Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds," International Journal of Scientific and Research Publications, vol. 3, no. 4, April 2013, ISSN 2250-3153.

[11] P. Pareek, "Cloud Computing Security from Single to Multi-clouds using Secret Sharing Algorithm," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 12, pp. 1-7, December 2013.

[12] M. A. AlZain, "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds," Journal of Software, vol. 8, no. 7, pp. 1-7, May 2013.

[13] B. Arun and S. K. Prashanth, "Cloud Computing Security Using Secret Sharing Algorithm," Paripex - Indian Journal of Research, vol. 2, no. 3, pp. 93-94, 2012, doi: 10.15373/22501991/MAR2013/35.

[14] S. Subashini and V. Kavitha, "A Survey on Security and Privacy Issues in Service Delivery Models of Cloud Computing," Journal of Networks and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[15] E. Dawson and D. Donovan, "The Breadth of Shamir's Secret Sharing Scheme," Computers & Security, vol. 13, no. 7, pp. 69-78, 1994.