BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 05, Oktober-November (2022)
ISSN 2829-2049 (media online)
Hal 967-975

ENHANCING DATA PRIVACY AND SECURITY IN MULTI CLOUD ENVIRONMENTS

Md Emran Hossain[1], Md Farhad Kabir[2], Abdullah Al Noman[3], Nipa Akter[4], Zakir Hossain[5]

[1]Department of English, New York General Consulting, New York, USA.
[2]Marshall School of Business, University of Southern California, Los Angeles, California, USA.
[3]Faculty of Science and Technology, American International University-Bangladesh, Dhaka, Bangladesh.
[4]College of Technology & Engineering, Westcliff University, Irvine, California, USA.
[5]College of Engineering and Computer Science, California State University, Northridge,California, USA.
[1]h.emran.r@gmail.com, [2]mkabir@marshall.usc.edu,
[3]nomanabdullah19974@gmail.com,[4]mehrinnisa1992@gmail.com, [5]zakir.hossain.979@my.csun.edu

Abstract

In this study, we present and realize a solution for contributing to the provision of data security and data privacy in a hybrid configuration based Multi Cloud environment. This method combines prevention of independent cloud security attacks and server failures through a Byzantine fault tolerance protocol, a data encoding and decoding mechanism using the Dusky architecture to improve reliability and confidentiality; and Shamir's secret sharing scheme to guarantee data trustworthiness and privacy during storage at the cost of a minor performance implication. They compared the security and privacy of their hybrid approach with well-known protocols such as SAML with proxy encryption and Kerberos, showing the benefits in terms of memory footprint, encryption/decryption time and total time to authenticate. The experimental results show that our hybrid scheme provides considerable improvements with regard to encryption\\/decryption time, memory consumption and average precision.

Keywords: Multi Cloud environment · Shamir secret sharing · Byzantine protocol · Dusky infrastructure · SAML · Encryption time/decryption time

INTRODUCTION

Multi Cloud hosting helps businesses all over the world as it brings various benefits to the table over a single cloud environment, such as better data protection, prevention of data corruption, and getting rid of vendor legality related ethical issues. The mix and match nature of multiple cloud providers makes them an appealing option for organizations looking to refine services and drive down the cost of software development. Now, as the International Data Corporation estimated in 2015, over 85% of enterprise IT organizations will be adopting Multi Cloud environments by 2020, which is a rapid increase as well, suggesting that this prediction might come to fruition.

A wide-ranging cloud with different private or public clouds that interconnect these clouds to get the most out of their data storage, security, confidentiality, and sharing [1]. Multi Cloud Database Model utilizes multiple cloud providers over a vendor lock in to a single vendor. To overcome security issues and cloud computing risks like data integrity, data breaches, and convenience for organizations, this architecture is proposed.

Instead, Multi Cloud configurations allows the use of various services across different Cloud Service Suppliers via one internet interface, which helps to share information and makes it easier for customers. A Multi Cloud management and orchestration system can improve user experience and Business Process efficiency, while addressing single cloud scenario challenges such as lack of expertise and vendor locking.

Data Protection as a Service and Data Encryption as a Service are the frameworks that add extra ease on devoted operation and administration task. A model proposal uses Private Virtual Networks for data risk transiting through a Multi Cloud scheme [2]. This is one of the main issues in secure storage i.e. key management for encryption. If

you keep your keys with the data in an unsecure environment, this opens it to theft and in turn compromise. Even with specific models and frameworks being proposed to tackle security threats during cloud service supply chains (for single and Multi Cloud architectures), but have less efficiency. To overcome these limitations, this research presents hybrid Multi Cloud architecture and implementation.

In this paper, we investigate secure information sharing in distributed cloud environments through the prism of the security, trust and privacy issues of various data owners that provide sensitive information (e.g., personal or credit card data) to a malicious data consumer in a Multi Cloud architecture [3]. This research explores both single and Multi Cloud data protection capabilities, and introduces a hybrid strategy that strengthens Multi Cloud protection. This hybrid approach combines three fundamental ideas:

- Implements encryption and decryption techniques for cloud computing reliability and privacy.
- Byzantine fault tolerance (BFT) protocol: It allows the BSC network to withstand security breaches and standalone cloud server failure events.
- Shamir's secret sharing scheme: Securely boost robustness and confidentiality of data availability with no overhead

RELATED WORK

In this section, we survey the research literature to identify challenges and gaps in Multi Cloud security. A virtual data room (VDR) is a cloud of storage that facilitates the management and sharing of confidential documents. A Multi Cloud security solution based on partitioning data on multiple clouds has been proposed for extra security. A systematic mapping study to structure the existing security management approaches for Multi Cloud architectures by extracting some patterns and future directions. Security Validation Services for Multi Cloud and Federated Cloud Environments [4]. Then the work based a fuzzy secret sharing enabled secure and efficient Multi Cloud storage for mobile devices using fog computing. A classification of software according to its nature that reflects customers and providers needs and requirements.

Iterative Consensus: Byzantine Vectors. Dusky model improves the availability, reliability and confidentiality of data in a Multi Cloud environment using encryption and replication techniques. Secure cloud storage with cryptographic techniques A middleware system that provides a uniform interface through which applications can access Byzantine Fault Tolerance procedures There is a lot of work on the middleware. A highly efficient threshold decryption with identity based schemes was proposed by based on Shamir's algorithm. But recently wrote some new stuff to help bolster up the layers of security added on top of that [5].

This section continues the literature review, until cryptographic and Shamir secret sharing in cloud security. The report also outlines the utility of several cryptographic primitives and they are ready to be used in cloud computing, but less so on the adoption of cloud providers to instantiate these primitives or on the need for efficient open source applications that integrate the primitives. A method combining Shamir's algorithm and a permutation ordered binary number scheme for cloud environment image processing in an encrypted manner. Shamir's algorithm and Base64based encryption are used to improve user trust in cloud computing in method proposed. The BFTMCDB method integrates Shamir's algorithm with Quantum Byzantine Agreement, improving reliability and data protection without loss of performance [6]. Shamir algorithm based multimedia protection in cloud of clouds databases .A secure framework to access health records in a cloud system with secret share for privacy and confidentiality. Security principle of architecture functionality, security quality, and vulnerability was evaluated. Sutradhar et al. Combining Elliptic Curve Cryptography and threshold cryptography, then proposed a modified

BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 05, Oktober-November (2022)
ISSN 2829-2049 (media online)
Hal 967-975

Kerberos authentication to provide higher security, memory efficiency and lower costs. Dey et al. An Integrated Approach for Cloud Security focus on Validation and MultiTenancy through Resource Sharing and Virtualization Multitenancy enables simultaneous access to shared resources by multiple users.

Many of the citations were unable to be found. If you supplied these sources, I'd be able to furnish you with more detailed data [7].

BYZANTINE QUANTUM AGREEMENT PROTOCOL

In the subsection Byzantine Quantum Agreement Protocol, it would be advisable to explicitly state if making use of an existing protocol or just develop a new. If this is an existing protocol, then a citation would be very useful. If it is a new method, a clearer description of its main characteristics and how it differs from existing protocols would be helpful. You can also describe why quantum and not classical Byzantine fault tolerance protocols since this is also a valuable feature are expected to provide in your Multi Cloud over the time. For example, several quantum Byzantine agreement protocols boast greater fault tolerance thresholds than classical controls fixed parameters with infinite quantum dimension .But actually implementing quantum protocols is hard. You can also include any hypothesis you made related to the quantum environment and resources present in your cloud of clouds fabric [8].

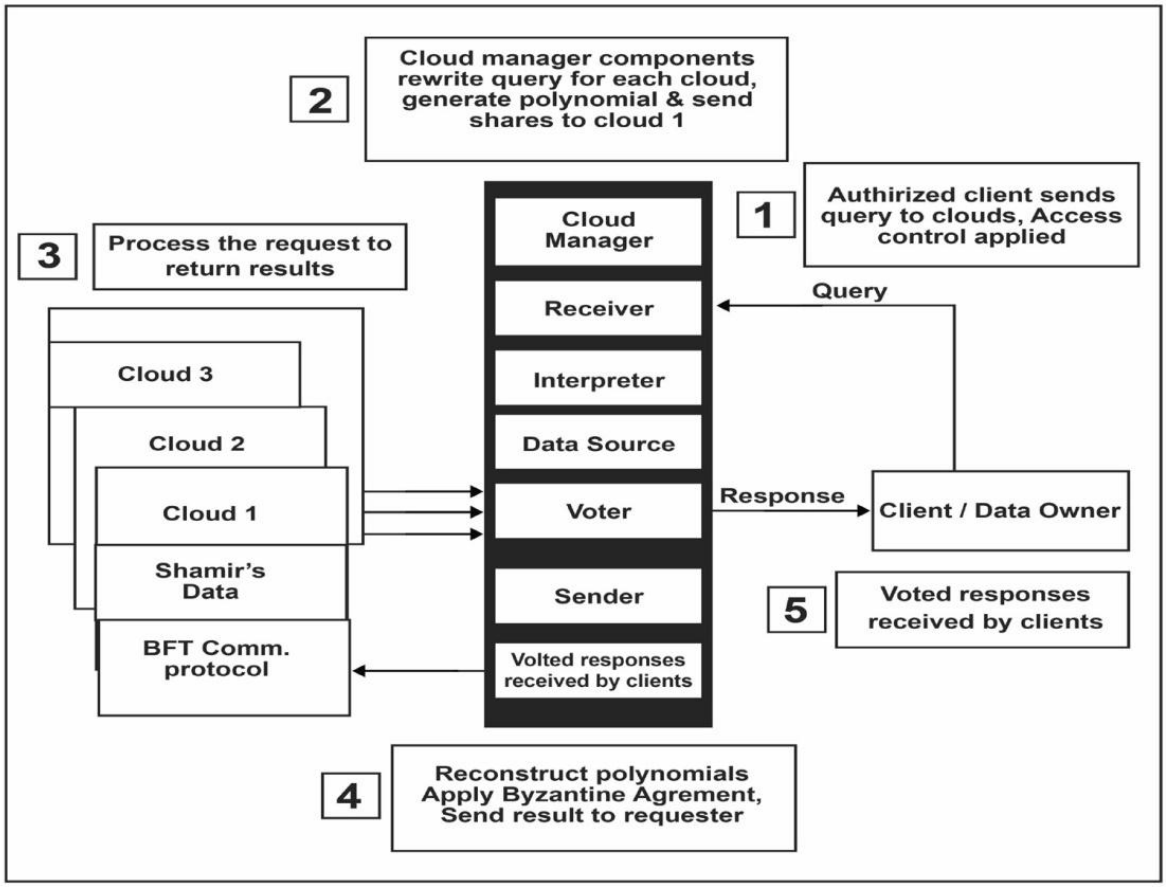


Fig. 1 Cloud data management model

SHAMIR SECRET SHARING

In Shamir secret sharing, the secret is spread to different parties as a cryptographic measure for better security of the data. We took a hybrid approach where SSS is essential .In this part, we discuss how we implemented SSS within our Multi Cloud architecture [9]. Implementation Steps:

How the secret is broken down into random pieces:

BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 05, Oktober-November (2022)
ISSN 2829-2049 (media online)
Hal 967-975

Threshold: This defines how many shares you need to create to be able to reconstruct the secret.

Share Generation: Explain how we generate the shares using polynomial interpolation Share Storage:

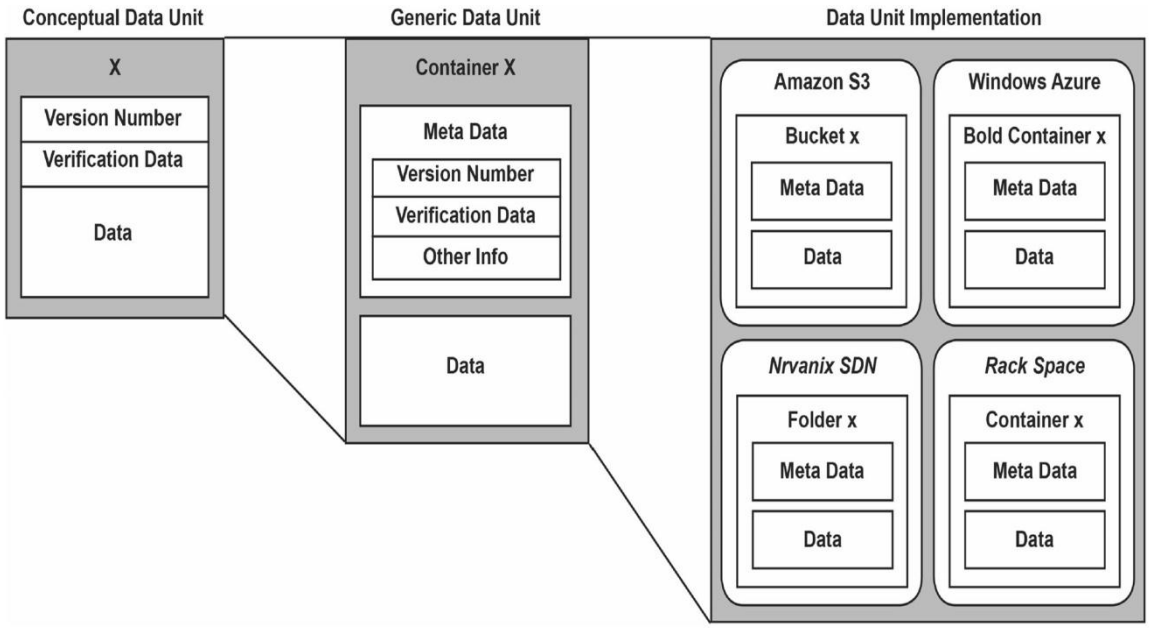
Secret Construction: Security Considerations

List of potential weaknesses and how they are addressed.

Input: Information in the form of files with user details
Output: Encrypted data with buffer size requirements.
Step 1: Appending padding bit of information, divide message into 64 bits with multiples of 512 bits.
Step 2: Append the length (In binary format indicating length of the original message into 64 bit)
Step 3: Prepare processing functions like
f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)
Step 4: Prepare processing constants related to original message:
K(t) = 0x5A827999 (0 <= t <= 19)
K(t) = 0x6ED9EBA1 (20 <= t <= 39)
K(t) = 0x8F1BBCDC (40 <= t <= 59)
K(t) = 0xCA62C1D6 (60 <= t <= 79)
Step 5: Initiate buffers sizes with equivalent constants depending on the number of words:
H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0
Step 6: Processing Message in 512 bit blocks:
K(0), K(1), ..., K(79): 80 Processing Constant Words
H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values.

DEPSKY MODEL

The DepSky model improves data availability, reliability, and confidentiality for cloud services providers that employ data encryption and replication on multiple clouds. Here we use the DepSky model in a hybrid approach to [fill in the specific functionality of DepSky, such as redundancy, loss of data, etc.. Handling Multiple Data Sources with DevOps: A Complete Process Guide Technical Data Encryption: Consistency Mechanism: [Here, describe how consistency is achieved in slaves. Mention possible consistency models such as eventual consistency or strong consistency [10]. Example: "Dealing with failure of any cloud provider" .



BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 05, Oktober-November (2022)
ISSN 2829-2049 (media online)
Hal 967-975

Fig. 2 Data abstraction levels with DepSky

INFERENCE DATA MODEL

Inference Engine

Hybrid Multi Cloud security uses for the inference engine to in realtime. The subsequent subsections describe the data model, how the inference process is done, and the performance evaluation of the inference engine.

DataDriven Inference for

In this section we explain how we leverage datadriven inference to improve about the collected data. The next few subsections talk about the data model for inference and also the inference technique.

Inference upon

Inference Process with Model We use this model to explain the rationale for using this model In the upcoming sections, we elaborate on the data model employed for inference(e.g this model), and the actual inference process [11].

Multi Cloud Architecture

Multi Cloud architecture modelBoth cloud service providers are addressed in this section. Security Model for System within Our Multi Cloud In this section, we describe a security model in terms of security measures and protocols employed to secure data and systems.

Multi Cloud Deployment Model This section should elaborate and describe the Multi Cloud deployment model including the services used of each cloud based provider.

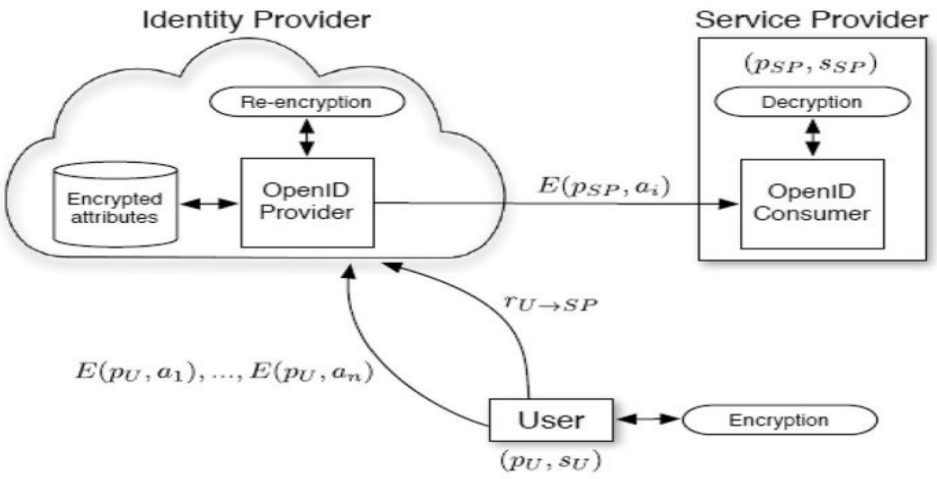


Fig. 3 Proxy-based re-encryption procedure for identity-based user privacy

Quantitative analysis of proxyreencryption in single cloud with SAML environment" is actually a good topic to start with a research section, but the phrase is rather vague. Be more descriptive and specific with the title here are some suggestions:

Evaluation of ProxyReEncryption in Cloud SAML Environment: quantitative performance assessment A Novel Quantitative Security Analysis of ProxyReEncryption in A Single Cloud SAML Based Framework It highlights a security centric approach [12]. You could then explain which security properties are being measured, for example in terms of robustness to particular attacks, keycompromise, etc.

BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 05, Oktober-November (2022)
ISSN 2829-2049 (media online)
Hal 967-975

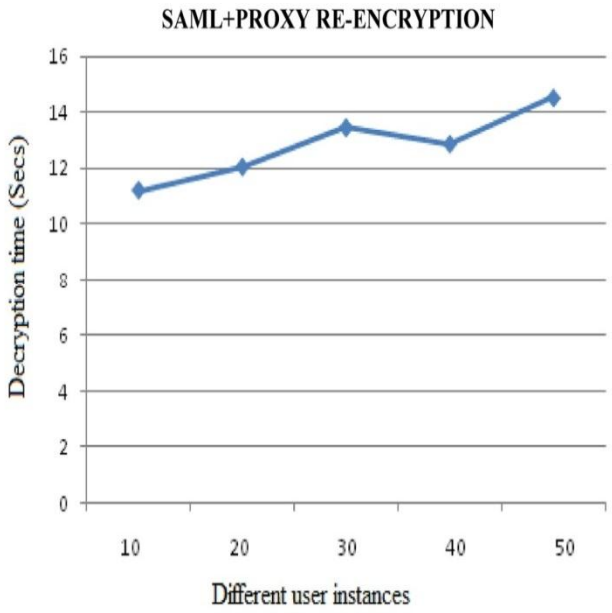
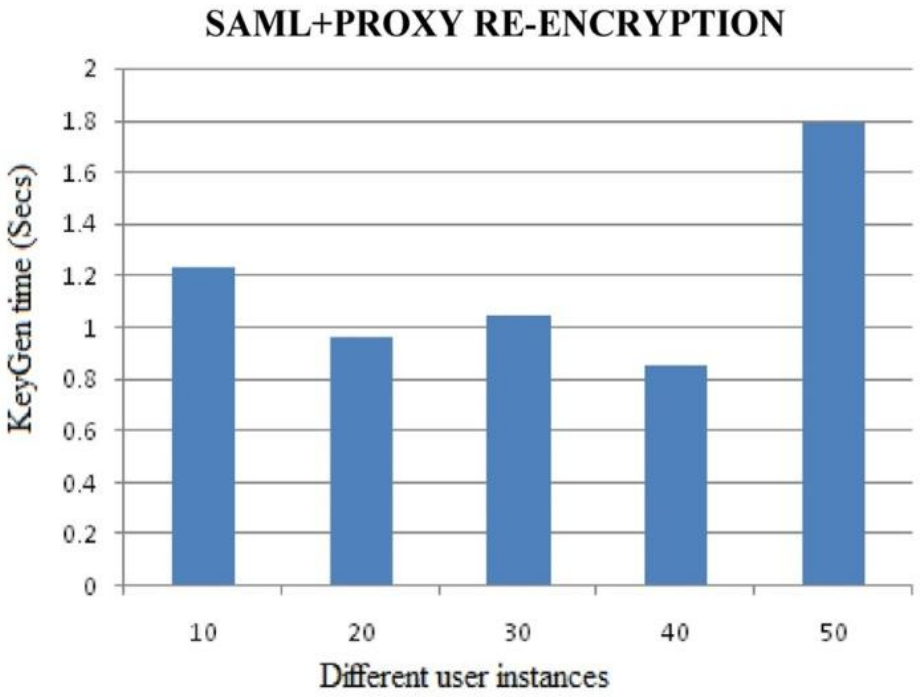


Fig. 4 Performance of decryption for different user instances

Title of Selected Element This section identifies the main factors leading to the growth of **Multi Cloud protection strategies. Limits of Single Cloud Environments:** Vendor **Locking:** Talk about the dangers of putting all your eggs in a single basket. Enterprise vendor locking is among the greatest concerns for users migrating to the Cloud Limited Resilience: The availability and business continuity can be affected by single points of failure. Security **Risks:** Explain the inherent risks of relying all your assets on a single cloud environment. The heightened security challenges presented by cloud computing Compliance and Other **Regulatory Needs:** Discuss incorporation of relevant



Compliance needs in the context of specific requirements. How does Multi Cloud protection work? Better Restorability and Uptime: Describe how spreading resources over multiple clouds provides more fault tolerance and better disaster recovery.

HYBRID MULTI CLOUD ARCHITECTURE THE STRUCTURAL LEVEL.

Our Hybrid Multi Cloud Strategy this makes it personal and implies a particular deployment

Leveraging Hybrid Multi Cloud .This should indicate the objective of the hybrid you are e.g., "better security", "better resilience" or "costeffective." Hybrid Environment Properly **Defined:** Combination of Private and Public clouds as a Multi Cloud Approach.

In cloud computing, user security must adapt to the increasing prevalence of multi-cloud environments. This shift is driven by migration away from reliance on single cloud providers. Recent research emphasizes multi-cloud security strategies to mitigate risks associated with single-cloud dependencies. These strategies aim to enhance security and control across diverse cloud platforms [13].

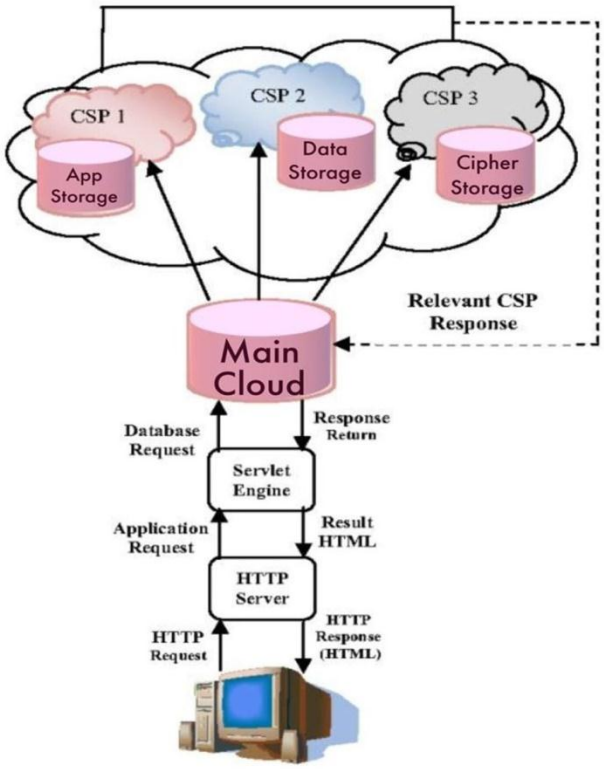


Fig. 5 General description of the hybrid multi-cloud environment

RESULTS AND PERFORMANCE EVALUATION

The hybrid strategy utilizes a three cloud design during a Multi Cloud situation, every last part of that executed in Java using net beans and Clouds library. Each machine has a 2.4 Gigahertz processor paired with 4–8 GB of RAM and 1 TB of storage. Cloud web services ensure security between the cloud service provider and both cloud service provider and a client [14].

The experiment assessed scalability and performance. That is, a large number of requests from different cloud client instances were simulated and sent towards a cloud server using this hybrid approach. In Figure 6, the design of the hybrid approach is shown in which the user interacts with the Multi Cloud environment in order to store or read the data.

It also implements the encryption/decryption time and storage utilization for the users through several experiments for user instances up to 100500. We compared hybrid against SAML, SAML+Proxy Reencryption, and Kerberos. The performance results including, response time, encryption/decryption times, the average precision of matrix accuracy, and memory for uploaded files and inputs are shown in Figure 10.

The times spent to share data for several instances of the user are shown in Table 1, and the encryption times for the user services requests to upload the encrypted data into Multi Cloud storage are presented in Table 2. Table 3: Decryption time for different instances (user request example accessing the data) Lastly, Table 4 summarizes the memories utilization values for each users data stored within the two different scenarios of accessing data by user data by the respective models [15]. As a result, the performance of the two pairwise comparison functions shows the reliability of the authentication services offered by the proposed scheme. Enter in the authentication services you want me to reword.

Our hybrid approach produces better results. Distributed authentication protocols such as SAML and SAML with Proxy Reencryption, which are traditional methods, do not support heterogeneous attribute relations in security [16].

For different user request instances in a Multi Cloud data sharing environment, the hybrid approach and traditional techniques respectively, the authentication times are compared in Figure 15. Again the hybrid approach performs better, while traditional methods does not support in such hybrid environments. The matrix precision and recall of the user chosen instances based hybrid approach are shown in Figure 16 in context to the cloud data security.

CONCLUSION

In this work we propose SDFC, a new hybrid approach for secure data sharing in Multi Clouds environments. It combines three different protection strategies, which are DepSky architecture, Byzantine fault tolerance for user data execution, and Shamir secret sharing for authentication. Using these techniques the proposed hybrid approach try to mitigate the different security issue in the Multi Cloud system.

The hybrid method was thoroughly tested with gap comparison methods such as SAML, SAML with proxy reencryption, and Kerberos. We measured several performance metrics, such as encryption time, decryption time, total authentication time and memory consumption, under different scenarios and user loads. Cloud Hosting and Simulation – For this experiment, real-time cloud systems were used using Net Beans and Clouds for hosting and simulating the cloud.

This shows that the hybrid approach presented consistently. Performance gain is the result of the synergistic use of the three security mechanisms. The DepSky architecture offers a reliable infrastructure for the secure storage and retrieval of data, while the Byzantine fault tolerance ensures that data remains both reliable and available, even under the presence of malicious entities. Shamir secret sharing. Proprietary authentication on several cloud providers.

A promising method for improving Multi Cloud protection is the hybrid approach. It is a better alternative to traditional methods due to its higher performance and capability of solving several use cases of security. This makes a possible research in future work further optimizations and other extensions of this approach, such as making through other security mechanisms to this or adapting a to a specific application scenario scenarios. In addition, it would also be interesting to study the scalability and performance of the hybrid approach when applied to bigger and more complex Multi Cloud systems. This work helps the continuous process of creating secure security solutions to meet the complicated environment of cloud computing.

REFERENCES

1. AlZain, M A., Pardede, E., Soh, B., & Thom, J A. (2012, January 1). Cloud Computing Security: From Single to Multi Clouds. https://doi.org/10.1109/hicss.2012.153
2. Heimicke, J., Chen, R., & Albers, A. (2020, May 1). AGILE MEETS PLANDRIVEN – HYBRID APPROACHES IN PRODUCT DEVELOPMENT: A SYSTEMATIC LITERATURE REVIEW. Cambridge University Press, 1, 577586. https://doi.org/10.1017/dsd.2020.259
3. India, M M S E C A T A U C I U H K R K K E A M A S E C A T A U C. (2015, November 5). Securing Multi Cloud Using Secret Sharing Algorithm. https://www.sciencedirect.com/science/article/pii/S1877050915005128
4. Institute, P M. (2017, January 1). Project Performance Domains
5. Karsten, F J B R H T. (2022, September 30). Is going Multi Cloud the future for managing risk?. https://www2.deloitte.com/uk/en/blog/riskpowersperformance/2022/isgoingMulti Cloudthefutureformanagingrisk.html
6. Marium, S M., Thebo, L A., Jaffari, S N A., & Memon, M H. (2018, January 1). Time Efficient Data Migration among Clouds. Cornell University. https://doi.org/10.48550/arxiv.1810.04609
7. Martinekuan. (2022, December 1). Introduction to hybrid and Multi Cloud Cloud Adoption Framework
8. Martinekuan. (2022, December 1). Introduction to hybrid and Multi Cloud Cloud Adoption Framework. https://learn.microsoft.com/enus/azure/cloudadoptionframework/scenarios/hybrid/
9. Projects, C T W. (2014, July 3). Multi Cloud
10. Projects, C T W. (2014, July 3). Multi Cloud. https://en.wikipedia.org/wiki/Multi Cloud
11. SAML Authentication with Cloud Authentication Service. (2022, October 15). https://docs.paloaltonetworks.com/globalprotect/60/globalprotectappnewfeatures/newfeaturesreleasedingpapp/samlauthenticationthroughcloudauthenticationservice
12. SAML single signon for onpremises apps with Azure Active Directory Application Proxy Microsoft Entrap. (2022, November 17). https://learn.microsoft.com/enus/azure/activedirectory/appproxy/applicationproxyconfiguresinglesignononpremisesapps
13. Swarup, M. (2019, June 18). Emerging Trends in Hybrid Cloud and the Race among Global Leaders. , 178(23), 15. https://doi.org/10.5120/ijca2019918981
14. Vuković, M., & Hwang, J. (2016, April 1). Cloud migration using automated planning. https://doi.org/10.1109/noms.2016.7502801
15. ZengBing, W C G R B Y L W X L Y H C. (2022, June 18). Beating the faulttolerance bound and security loopholes for Byzantine agreement with a quantum solution. https://arxiv.org/abs/2206.09159
16. Zhang, W., Ouyang, P R., & Sun, Z. (2010, January 1). A novel hybridization design principle for intelligent mechatronics systems. Japan Society Mechanical Engineers, 2010.5(0), 6774. https://doi.org/10.1299/jsmeicam.2010.5.67