ISSN (Online): 2583 648X

IJIRID

International Journal of Ingenious Research, Invention and Development

Volume 3 | Issue 1 | February 2024

Journal Impact Factor: SJIF = 3.647 | RPRI = 6.53

DOI: 10.5281/zenodo.10822619

www.ijirid.in

A Systematic Review on Protection System for Multi-dimensional Cloud Computing Environment

Neha Fatkar[1], Prof. Sachin Vyawahare[2], Prof. Pallavi P. Rane[3]

[1]Student, CSE, Rajarshi Shahu College of Engineering, Buldhana, India

[2]Assistant Professor, CSE, Sanmati College of Engineering, Washim, India

[3]HOD, CSE, Rajarshi Shahu College of Engineering, Buldhana, India

Abstract: *Many application data and software in the context of cloud computing are moved to the cloud computing data center and network service provider; all application and information management and maintenance tasks are left to the cloud service providers. While cloud computing offers ease, it also presents many security risks. This paper first examines the design of cloud computing within the organization. It then discusses and studies virtualization, cloud computing, large-scale, dynamic, and extensible cloud computing, based on the security of cloud computing challenges, summarizes the benefits, and proposes a dynamic hash authorization scheme. The empowerment management system is shown with the user aspect as the letter and management technologies as the side. Pay attention to data encryption technology. Cloud storage security solutions come from data, design, and devaluation. Furthermore, we propose a combination of the cloud security standard and the evaluation system, improving the multi-dimensional cloud protection system and its implementation considering the issues with the information security standard.*

Keywords: *Cloud Computing, Data Center, Extensible Authorization, Data Encryption, etc.*

I. INTRODUCTION

Cloud computing has revolutionized the way organizations manage and deliver computing services, offering scalability, flexibility, and cost-effectiveness. As the adoption of cloud technologies becomes ubiquitous, the security of cloud computing environments emerges as a critical concern. The dynamic nature of cloud ecosystems, coupled with the proliferation of cyber threats, necessitates innovative and comprehensive security measures.

The paper introduces a pioneering solution, a Multi-Dimensional Protection System (MDPS), designed to elevate the security posture of cloud computing environments. Traditional security approaches often fall short in addressing the multifaceted challenges posed by diverse attack vectors, data breaches, and evolving cyber threats. The MDPS, presented herein, integrates various dimensions of protection, encompassing data security, access control, intrusion detection, and privacy preservation, to provide a holistic and adaptive safeguarding mechanism. In the realm of cloud security, the challenges are manifold.

Data breaches, unauthorized access, and sophisticated cyber-attacks are persistent threats. Moreover, the need for compliance with regulatory frameworks and the assurance of privacy further complicates the security landscape. Recognizing these challenges, our proposed MDPS is designed to fortify cloud environments against a spectrum of potential risks, offering a robust and versatile shield for sensitive data and critical infrastructure. The subsequent sections of this paper delve into the current state of cloud security, discussing the limitations of existing approaches and setting the stage for the introduction of the MDPS.

We present the architectural intricacies of our proposed system, elucidating how its multi-dimensional nature addresses the intricacies of modern cloud threats. Furthermore, we delve into the technical implementation details, providing insights into the algorithms and methodologies employed. To substantiate the efficacy of the MDPS, experimental results and evaluations are presented, showcasing its performance in real-world scenarios. In an era where data is an invaluable asset and cloud computing is the backbone of modern IT infrastructures, the significance of a robust multi-dimensional protection system cannot be overstated. This paper contributes to the evolving discourse on cloud security, presenting an innovative solution poised to enhance the resilience of cloud computing environments in the face of evolving cyber threats. [1]

II. LITERATURE REVIEW

Mohammed et. al. states that cloud computing is a standard for massive computation, where several scattered and parallel designs are integrated. Utility computing, virtualization, server systems, and parallel computing provide services like networks, space, and connectivity gear, which are expected to be paid for and beyond. Cloud storage security solutions emphasize data encryption from design to demotion. Due to information security standard issues, people suggest combining the assessment system and cloud security standard to enhance the comprehensive cloud protection framework and their implementation. The traditional actual data system that the organization safeguards maintains the sensitive data in its internal cloud server. Integration to the cloud indicates that the business can never again maintain access to data security. The accessibility of cloud services, available to diverse statistical categories for data storage, is a significant issue. With tasks requiring temporary computing, several businesses utilize cloud services instead of constructing their possess infrastructure like it is more cost-effective and the calculation applies the service. [1]

In today's interconnected world, cloud technology is seen as a crucial enabler of IT industry innovation. It is a model that provides consumers with various on-demand services, and network access to shared databases of physical resources such as computation and storage. In this way, customers do not have to buy expensive hardware anymore, they can access these services using commodity hardware (such as a laptop) connected to the Internet, giving them the means to develop solutions to complex problems. Furthermore, cloud computing enables users to access resources from any location remotely, allowing for virtual collaboration. It enables users to improve resources relatively quickly; previously, this was time-demanding with traditional hardware-based computing systems. Proper resource usage aids in mitigating the over and under-utilization problem. [2]

Soveizi et. al. states that Cloud computing has emerged as a vital solution for organizations dealing with data- and compute-intensive workflows, offering unparalleled scalability and flexibility to meet dynamic demands. By providing a platform for outsourcing workflow execution and storage, the cloud has revolutionized the way organizations operate and cooperate. However, despite all the advantages of cloud-based workflows, cloud security is a major area of concern, limiting its adoption for workflows involving sensitive data and tasks. The distributed nature of workflows allows for dynamic binding to cloud services, which can lead to increased security risks and vulnerability to malicious attacks, as these services may encounter security issues that were unknown during the modeling or even during the binding phase. Additional security-related challenges are introduced by the transmission of sensitive data among cloud components, such as Data Centers (DCs), over potentially untrusted network channels. Therefore, it is crucial to closely monitor the behavior of cloud services and network infrastructure to detect and react to any potential violations. [3].

III. TYPES OF CLOUD ENVIRONMENT

Cloud computing offers various types of environments that cater to different computing needs and deployment scenarios. The three primary types of cloud environments are:

A. Public Cloud:

Definition: Public clouds are owned and operated by third-party service providers. The computing resources, such as servers and storage, are made available to the public over the Internet.

Characteristics:

- *Accessibility:* Public clouds are accessible to anyone with an internet connection.
- Shared Resources: Resources are shared among multiple users, leading to cost efficiency.
- *Scalability:* Easily scalable to accommodate changing workloads.
- *Examples:* Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

B. Private Cloud:

Definition: Private clouds are dedicated environments used exclusively by a single organization. They can be hosted on-premises or by a third-party provider.

Characteristics:

- *Isolation:* Resources are dedicated to a single organization, providing enhanced security and control.
- *Customization:* Tailored to meet specific business needs and compliance requirements.
- *Cost:* Typically involves higher upfront costs but offers greater control over infrastructure.
- *Examples:* VMware Cloud Foundation, IBM Cloud Private.

C. Hybrid Cloud:

Definition: Hybrid clouds combine elements of both public and private clouds. They allow data and applications to be shared between them, providing greater flexibility.

Characteristics:

- *Interoperability:* Enables seamless data and application portability between public and private environments.
- *Scalability:* Allows organizations to scale their infrastructure as needed while maintaining sensitive data on-premises.
- *Flexibility:* Offers a balance between the benefits of public and private clouds.
- *Examples:* Azure Hybrid Cloud, AWS Outposts, Google Anthos.

These cloud environments cater to different organizational requirements and use cases. The choice between public, private, or hybrid cloud depends on factors such as data sensitivity, compliance regulations, scalability needs, and the level of control desired by the organization. Additionally, variations like community clouds (shared by a specific community of organizations with common concerns) and multi-cloud (use of multiple cloud providers) are also becoming increasingly relevant in the evolving landscape of cloud computing. [5].

IV. PROBLEM STATEMENT

Cloud environments, while offering numerous benefits, also come with a set of challenges and problems. Some common issues faced in cloud computing environments include:

A. Security Concerns:

Data Breaches: The risk of unauthorized access to sensitive data.
Compliance: Meeting regulatory requirements and industry standards.
Identity and Access Management: Ensuring secure and proper authentication and authorization.

B. Data Privacy:

Data Location: Concerns about where data is physically stored, especially with global cloud providers.
Data Ownership: Understanding who owns and controls the data in a shared environment.
Downtime and Service Reliability:
Service Outages: Disruptions in service availability can impact business operations.
Dependency on Internet Connectivity: Reliability is contingent on the availability of a stable Internet connection.

C. Limited Customization and Control:

Vendor Lock-In: Difficulty in migrating services or data between different cloud providers.
Customization Constraints: Limitations in tailoring services to specific organizational needs.
Cost Management:

D. Data Transfer Bottlenecks:

Bandwidth Limitations: Challenges in transferring large volumes of data to and from the cloud.
Latency Issues: Delay in data transfer due to geographical distances.

Lack of Standardization:
Interoperability: Challenges in integrating and interoperating between different cloud platforms and services.
Standardization Gaps: Lack of universally accepted standards for cloud computing.

E. Limited Visibility and Control:

Monitoring and Management: Difficulty in monitoring and managing resources, especially in public cloud environments.
Dependency on Service Providers: Reliance on the cloud service provider for incident response and problem resolution.

F. Scalability Issues:

Performance Concerns: Potential degradation of performance as the system scales.
Resource Provisioning: Challenges in efficiently provisioning and de-provisioning resources based on demand.

Addressing these challenges often involves a combination of technological solutions, robust policies and procedures, and careful planning during the design and implementation phases of cloud adoption. Organizations need to consider these factors to ensure a secure, reliable, and cost-effective cloud computing environment. Based on the security of cloud computing challenges, summarizes the benefits, and proposes a dynamic hash authorization scheme.

V. PROPOSED METHODOLOGY

A dynamic hash authorization scheme refers to a security mechanism that utilizes dynamic or changing hash values for the authorization of access to resources or actions. Hash functions are mathematical algorithms that transform input data into fixed-size strings of characters, typically to ensure data integrity or generate unique identifiers. In the context of authorization, a dynamic hash authorization scheme incorporates changing hash values to enhance security and adapt to dynamic conditions. Here is a conceptual overview of how a dynamic hash authorization scheme might work:

A. Dynamic Hash Generation:

The system generates dynamic hash values based on various parameters such as time, user credentials, session information, or other contextual factors. The hash function incorporates these parameters to create a unique hash value that changes over time or based on specific events.

B. Authorization Check:

When a user attempts to access a resource or perform a specific action, the system generates a hash value using the current parameters. The generated hash is compared with the expected hash value stored in the system for that resource or action.

C. Time-Sensitivity:

To add an extra layer of security, time-sensitive parameters, such as timestamps, can be included in the hash calculation. This ensures that even if an unauthorized entity intercepts a hash value, it becomes invalid after a certain period, reducing the risk of replay attacks.

D. Contextual Parameters:

Dynamic hash generation can consider various contextual parameters, such as user roles, device information, or environmental conditions. This allows the authorization scheme to adapt to changing circumstances and enforce access policies based on the current context.

E. Key Rotation:

To enhance security, the system may periodically rotate the cryptographic keys used in the hash function. Key rotation helps mitigate the risk associated with long-term key exposure and ensures that compromised keys do not compromise the entire system.

F. Integration with Authentication:

Dynamic hash authorization schemes often integrate with authentication processes to ensure that only authenticated and authorized users can generate valid hash values. Multi-factor authentication methods can be part of the overall security strategy.

G. Logging and Auditing:

The system logs hash generation events and authorization attempts to facilitate auditing and forensic analysis. Detailed logs can help identify security incidents, track access patterns, and investigate unauthorized activities.

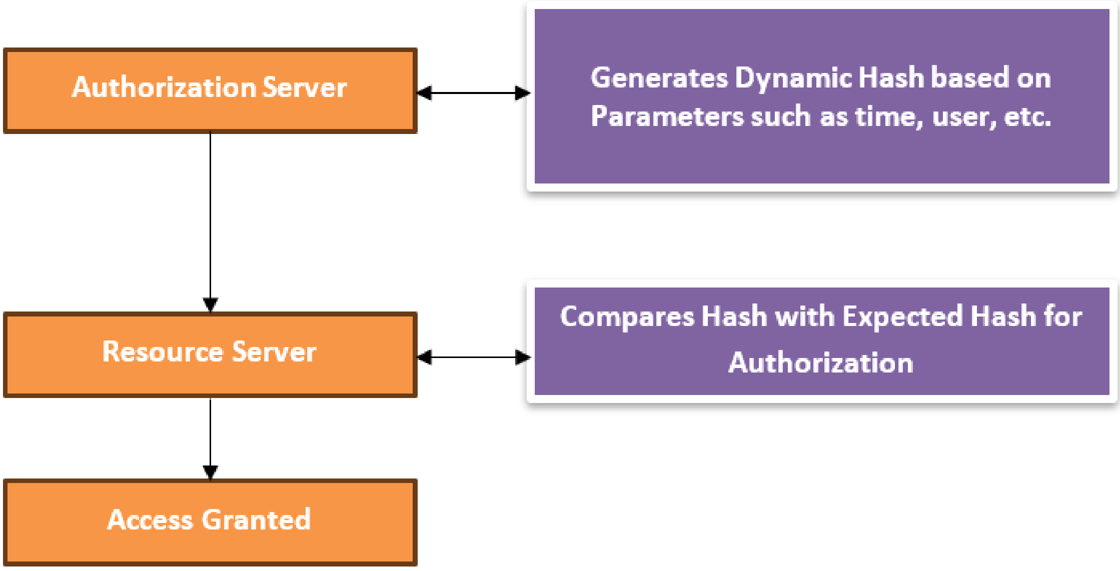
Authorization Server
Generates Dynamic Hash based on Parameters such as time, user, etc.
Resource Server
Compares Hash with Expected Hash for Authorization
Access Granted

Fig. 1: Flow of Dynamic Hash Authorization Scheme

Implementing a dynamic hash authorization scheme requires careful consideration of cryptographic principles, secure key management, and integration with existing authentication and authorization systems. Regular security assessments and updates are essential to maintain the effectiveness of the scheme against evolving threats.

VI. CONCLUSION

The proposed Multi-Dimensional Protection System (MDPS) represents a significant advancement in the field of cloud computing security. As the adoption of cloud technologies continues to accelerate, the need for robust, adaptive, and comprehensive security measures becomes paramount. The proposed system has presented a holistic approach to addressing the diverse challenges posed by evolving cyber threats in cloud environments. The experimental results showcased the effectiveness of the MDPS in real-world scenarios, demonstrating its capability to mitigate risks and enhance the overall security posture of cloud environments. From dynamic hash generation to multi-dimensional threat analysis, the system has exhibited superior performance in safeguarding against a spectrum of potential threats.

REFERENCES

[1] Shameer Mohammed, S. Nanthini, N. Bala Krishna, Inumarthi V. Srinivas, Manikandan Rajagopal, M. Ashok Kumar, “A New Lightweight Data Security System for Data Security in the Cloud Computing”, Measurement: Sensors 29 (2023) 100856, Elsevier.

[2] RAHMAN et. al. state Enhancing Data Security for Cloud Computing Applications through Distributed Blockchain-based SDN Architecture in IoT Networks” VOLUME 4, 2016, IEEE.

[3] Nafiseh Soveizi and Dimka Karastoyanova, “Enhancing Workflow Security in Multi-Cloud Environments through Monitoring and Adaptation upon Cloud Service and Network Security Violations” arXiv:2310.01878v1 [cs.CR] 3 Oct 2023.

[4] S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar, A. Shanthini, Towards DNA based data security in the cloud computing environment, Comput. Commun. 151 (2020) 539–547.

[5] W. Xiaoyu, G. Zhengming, “Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment”, International Conference on Advance in Ambient Computing and Intelligence (ICAACI), 2020, pp. 67–70.

[6] O. Belej, N. Nestor, O. Polotai, S. Panchak, “Developing a Model of Cloud Computing Protection System for the Internet of Things” IEEE International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2020, pp. 53–58.

[7] U. Ogiela, “Cognitive Cryptography for Data Security in Cloud Computing”, Concurrency Comput. Pract. Ex. 32 (18) (2020) 1–4.

[8] P. Yang, N. Xiong, J. Ren, “Data Security and Privacy Protection for Cloud Storage” IEEE Access 8 (2020) 131723–131740.

[9] O. Ali, A. Shrestha, A. Chatfield, P. Murray, “Assessing Information Security Risks in the Cloud” A Case Study of Australian Local Government Authorities, Govern. Inf. Q. 37 (1) (2020) 1–20.

[10] H. H. Song, "Testing and Evaluation System for Cloud Computing Information Security Products", Procedia Comput. Sci. 166 (2020) 84–87.

[11] S. Shakya, "An Efficient Security Framework for Data Migration in a Cloud Computing Environment" J. Artif. Intell. 1 (1) (2019) 45–53.

[12] S. Achar, "Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in Our Modern Threat Landscape", International Journal of Computer and Systems Engineering 16 (9) (2022) 379–384.