RESOURCE OPTIMIZATION IN CLOUD COMPUTING FOR PAYG USING SHA-256

Sathya S[1], Keerthana A J[2], Balavidhya G[3], Sivaramakrishnan R[4]

[1] Assistant Professor, Computer Science and Engineering, Hindusthan College of Engineering and Technology, Tamil Nadu, India
[2] Student, Computer Science and Engineering, Hindusthan College of Engineering and Technology, Tamil Nadu, India
[3] Student, Computer Science and Engineering, Hindusthan College of Engineering and Technology, Tamil Nadu, India
[4] Student, Computer Science and Engineering, Hindusthan College of Engineering and Technology, Tamil Nadu, India

ABSTRACT

Cloud computing offers on-demand access to computing resources over the Internet, with providers offering services at reasonable prices and using various pricing models to reflect different quality levels. One approach to these pricing schemes is k-times anonymous authentication (k-TAA), which ensures access control, user anonymity, and public traceability. In k-TAA, users can anonymously access services up to k times; exceeding this limit makes their actions traceable. This scheme acts as a prepaid plan based on access frequency.
Alternatively, the pay-as-you-go (PAYG) model charges users based on actual usage, minimizing unnecessary costs. Integrating k-TAA with PAYG sets the access bound k by the prepayment amount, but current k-TAA schemes only allow single access per authentication, making them impractical.

To address this, we propose a new k-TAA primitive called k-times anonymous pay-as-you-go authentication (k-TAA-PAYG), allowing multiple accesses per authentication session within the limit k. The proposed system dynamically allocates resources based on real-time demand, monitored through user access patterns and usage metrics, thus maximizing resource utilization and minimizing costs.SHA-256-based framework significantly improves the accuracy and security of resource allocation while maintaining low computational overhead. This ensures that users are charged accurately based on actual usage, and providers can optimize their resource distribution effectively. This study highlights the potential of cryptographic techniques in enhancing cloud computing resource management and security.

Keyword: *Networks, Security, Cloud Computing , RESOURCE ALLOCATION , SECURE HASH FUNCTION 256*

---

1. INTRODUCTION

A pay-as-you-go (PAYG) model in cloud computing allows users to pay for application, platform, service, and computing resources based on usage. Quality of Service (QoS) aspects like performance, availability, and reliability, detailed in Service Level Agreements (SLAs), measure service performance. Cloud computing ensures data and hardware availability to authorized users. However, it is vulnerable to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which aim to disrupt services and consume system resources, rendering them inaccessible.

DDoS attackers exploit cloud features like PAYG, auto-scaling, and multi-tenancy, leading to high resource consumption and costs. For instance, Amazon EC2 faced significant disruptions due to a DDoS attack. Defense strategies include proactive measures like challenge-response and restrictive access, and reactive measures like anomaly detection and resource usage monitoring. Attack mitigation techniques include victim migration and Software Defined Networking (SDN). DDoS attacks not only violate SLAs but also increase CPU and memory usage, indirectly raising energy consumption.

2. MODULES

- Resource Management Module
- Billing and Metering Module
- Authentication and Authorization Module
- Load Balancing Module
- Encryption and Security Module
- Monitoring and Reporting Module

2.1 Resource Management Module

This module is responsible for managing the available resources in the cloud environment. It includes functions such as resource provisioning, monitoring, and scaling to ensure that resources are allocated efficiently based on demand.

2.2 Billing and Metering Module

This module tracks resource usage by individual users or applications and calculates the associated costs. It includes functionalities such as metering usage, generating invoices, and providing cost breakdowns to users.

2.3 Authentication and Authorization Module

Security is paramount in cloud computing. This module ensures that only authorized users or applications can access resources and perform operations within the cloud environment. Authentication verifies the identity of users, while authorization controls the actions they can perform.

2.4 Load Balancing Module

In a cloud environment, multiple resources are often available to handle incoming requests. The load balancing module distributes incoming traffic across these resources to optimize performance, prevent overload, and ensure high availability.

2.5 Encryption and Security Module

While SHA-256 can be part of this module for ensuring data integrity and authenticity, it's just one component. This module handles encryption of data in transit and at rest, as well as implementing security protocols to protect against unauthorized access and data breaches.

2.6 Monitoring and Reporting Module

This module provides real-time monitoring of resource usage, performance metrics, and system health. It generates reports and alerts administrators or users about any anomalies or issues that require attention.

3. FLOWCHART DIAGRAM

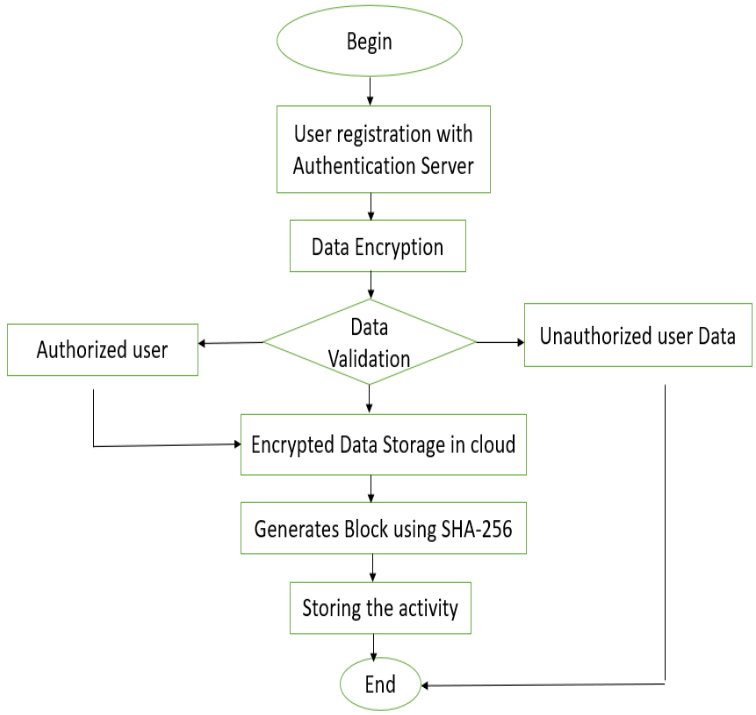

Fig. - 1: Flowchart

4. SYSTEM ARCHITECTURE

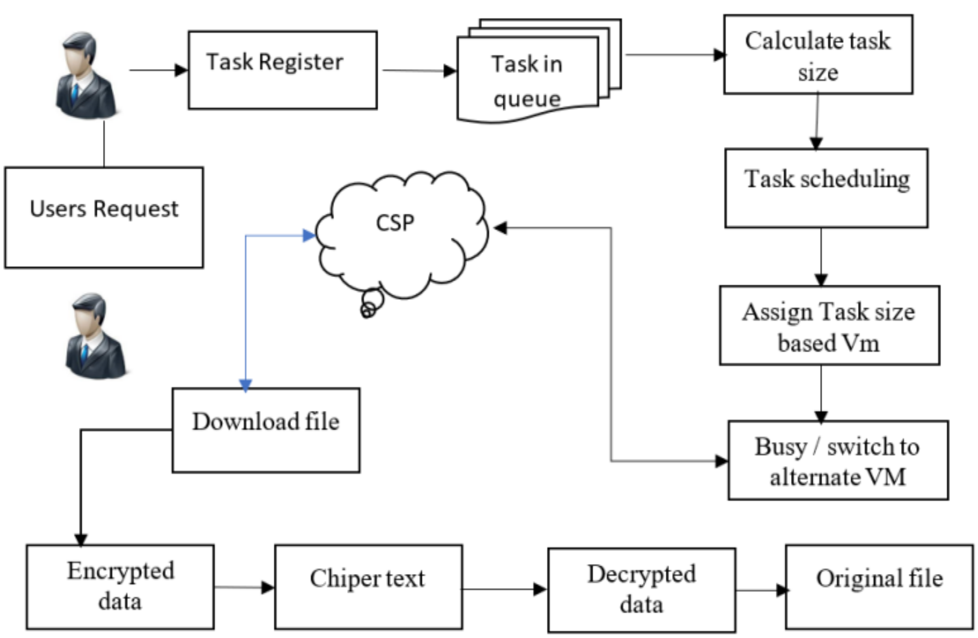

Fig. -2: Architecture Diagram

5. RESULTS

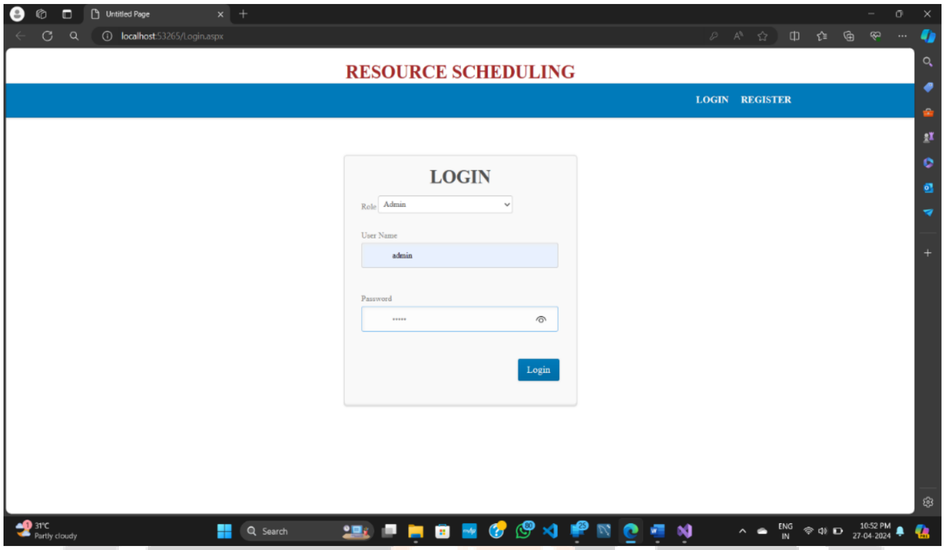

Fig-3 ADMIN LOGIN

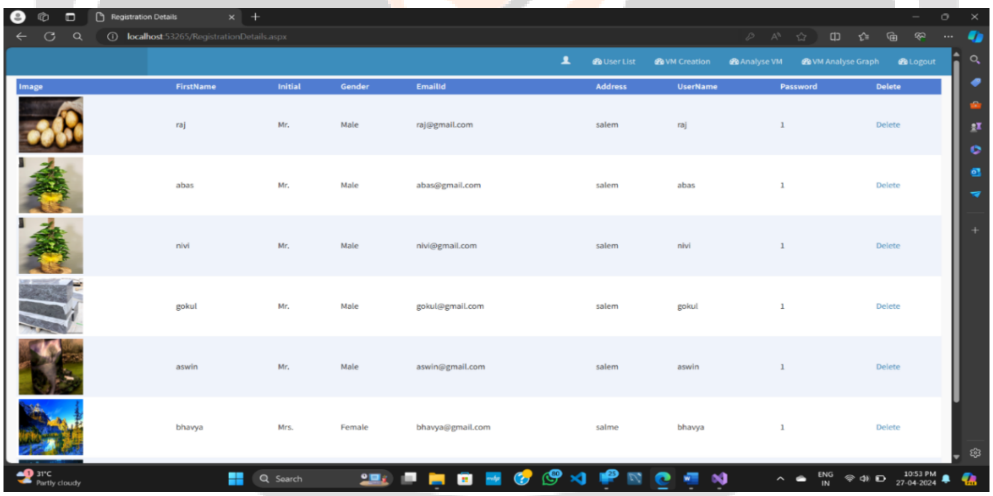

Fig-4 USER LIST

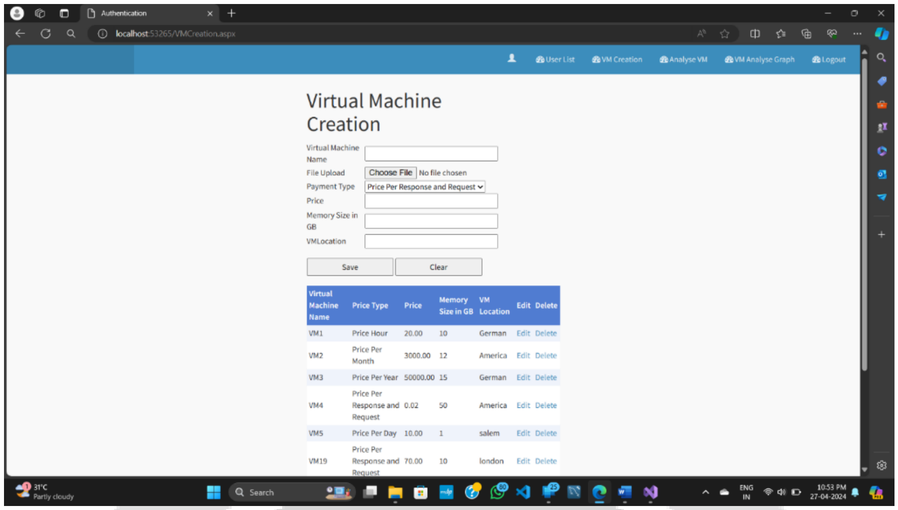

Fig -5 VIRTUAL MACHINE CREATION

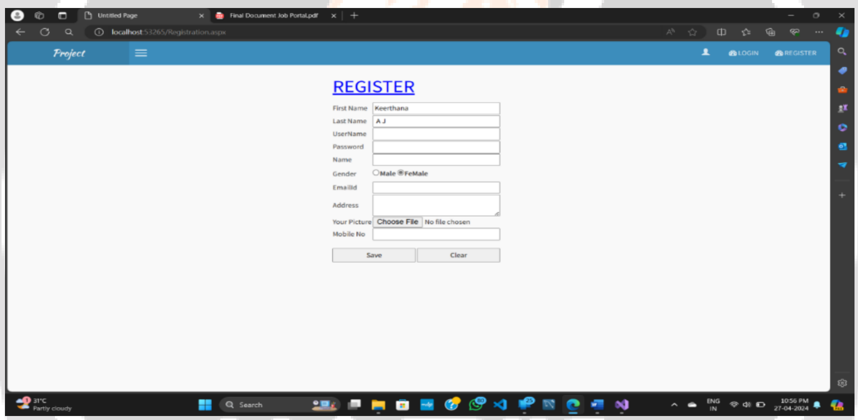

Fig-6 USER REGISTRATION

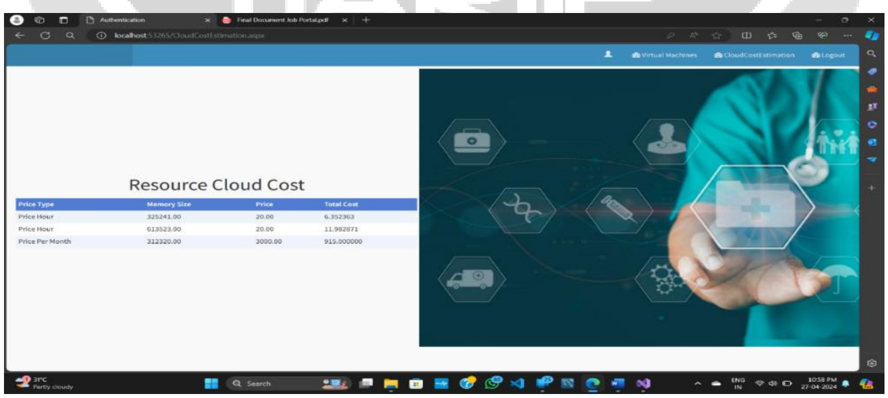

Fig – 7 Cloud cost Estimation

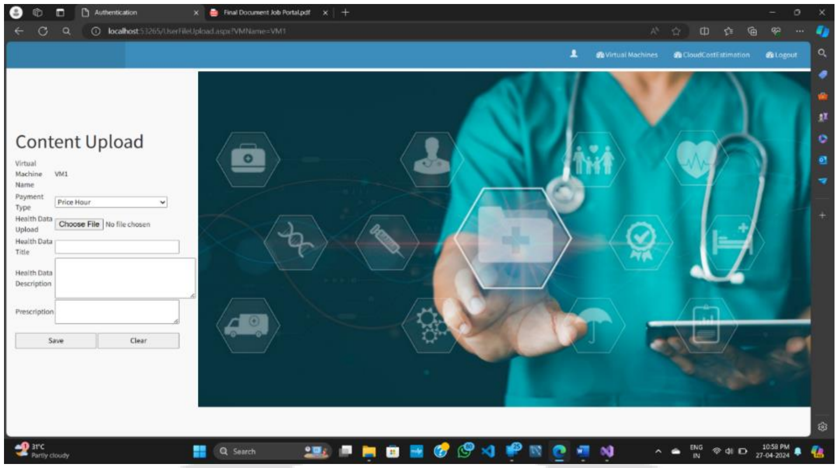

Fig-8 Data Upload

6. CONCLUSION

A network storage security scheme that collectively deals with the security and performance in terms of retrieval time. Thus, authors propose an anonymous but secure authentication scheme for the data stored in cloud. User revocation is done and once a user is relocated cannot view the messages stored on the cloud. This system can be useful for government and non government organizations. Our aim is to promote paperless work.

7. REFERENCES

[1]. Teranishi, J. Furukawa, and K. Sako, "k-times anonymous authentication (extended abstract)," in Advances in Cryptology ASIACRYPT 2004. Springer, 2004, pp. 308–322.

[2] D. Chaum, "Blind signature system," in Advances in cryptology. Springer, 1984, pp. 153–153.

[3] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in Annual International Cryptology Conference. Springer, 2000, pp. 255–270.

[4] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2003, pp. 614–629.

[5] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in International Workshop on Public Key Cryptography. Springer, 2005, pp. 416–431.