WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Optimized and Secured Application Delivery Service in Cloud

[1]Dr. Rais Abdul Hamid Khan, [2]Dr. Rajeev Kumar Arora, [3]Yogesh Kantilal Sharma, [4]Dr. Mohammad Muqeem,

[1]Professor, SOCSE, Department of Computer Science & Engineering Sandip university. Nashik, India. rais.khan@sandipuniversity.edu.in

[2] Programmer Analyst, Department of Information Technology, Nicklaus Children's Hospital, Miami, USA rajeev04.study@gmail.com

[3]Assistant Professor, Department of Computer Engineering Department, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India yogesh.sharma@viit.ac.in

[4] Professor, SOCSE, Department of Computer Science & Engineering, Sandip university. Nashik, India. Muqeem.79@gmail.com

ABSTRACT

With cloud computing, resources such as storage and computation are hosted in a centralized location and made accessible through an internet connection to many users on demand. It's a method of accessing a shared pool of computer resources on-demand from any locale with little administrative effort. Private and public clouds are now viable options for users and enterprises of all sizes to store and process data (Third party server). Data access methods are simplified and made more reliable with an internet connection. It may be done anytime and anywhere at a reduced price. When discussing what is meant by "cloud computing," it's important to distinguish between the various service types (SaaS, PaaS, IaaS, SEaaS), features (On-demand service, Broad Network Access, Resource pooling, Rapid Elasticity, Measured Service), and deployment strategies (Public, Private, Community, Hybrid, and Mobile Cloud). The Cloud's flexibility has led to a mass exodus of data. A fundamental challenge for present-day cloud computing storage infrastructures is providing highly secure and efficient data access. Users are drawn to cloud storage for the considerably expanded capacity it provides. Thus data security must be a top priority. A severe security risk arises when private information is stored off-site outside the user's reach. Due to the vulnerability of data during transmission and storage, data security is crucial. Several different algorithms may be used for cryptography. Data encryption techniques exist, including DES, AES, and Triple DES. In symmetric critical approaches, the key is utilized for both encryption and decryption. In contrast, RSA, ECC, and homomorphic equations are examples of asymmetric cryptosystems, which need two separate keys for encryption and decryption. However, these algorithms can be broken by anybody with enough time and effort. Therefore, it's crucial to improve cloud storage security. This research aims to improve the safety and efficiency of application delivery services hosted on the Cloud.

Keywords: Application Delivery Service, Application Security, Secure Cloud, Cloud Application, Optimized Application.

1. Introduction

The term "cloud computing" refers to a service delivery model in which users have near-constant, anywhere-access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with little to no management effort or interaction from the service provider. This cloud architecture has three types of services and four types of deployments [1]. IaaS, PaaS, and SaaS are the three primary service paradigms in cloud computing, sometimes used interchangeably [2]. Cloud computing has gained much popularity because of the ease of data transmission. As technology advances, the potential threat to the cloud environment is also increasing. So it is necessary to secure the data travelling to and from the Cloud. McAfee found that the rate of cyber assaults on Cloud infrastructure has surged by an alarming 630 per cent since 2020 [3]. In contrast, the usage of cloud services has increased by 50%. Data security is crucial while simultaneously delivering efficient and optimized services. This paper provides a model for secure and optimized delivery service for cloud environments. There are many securing algorithms for securing the data. We are going to use Enhanced AES encryption for our model. This encryption mechanism used features like critical scheduling, Substitution-Permutation network and hardware acceleration. To Reduce the redundancy of data or repetition of the same file, we will use hashing algorithms like SHA256 to generate a hash of each file and store them to avoid duplication of the same file. This model will also implement load-balancing techniques for controlling the incoming traffic to make it more efficient and optimized. The load-balancing methods include caching and content delivery networks.

2. Literature Survey

Gupta et al. [4] presented a two-level load-balancing architectural approach for cloud settings, as shown in Figure 1. Our investigation is based on this approach, which includes distributing workloads between Physical Machines (PMs) and Virtual Machines (VMs). It incorporates intra-VM and inter-

VM task migration sets to achieve workload balance. Our work builds upon Gupta et al.'s model, explicitly exploring application delivery services with optimization and enhanced security.Regarding content distribution and access, the Internet has limits, and CDNs (Content Delivery Networks) have evolved to solve these problems. With conventional CDNs, data is replicated over a network of cache servers worldwide, and client requests are redirected depending on various web and service-related factors. However, a cloud-oriented content delivery network (CCDN) uses the Cloud to its advantage for scalable capacity and lower development costs, making it the CDN of the future. Integrating CDNs with cloud computing, specifically within a networked cloud environment (NCE), presents challenges regarding resource mapping, surrogate placement, and efficient content distribution across multiple administrative domains. While traditional CDN research provides insights, a cloud-based CDN requires unique considerations. This proposed work aims to address these challenges and contribute to the advancement of CCDNs [5]. Coppolino et al. [6] have mentioned the major security issues of the Cloud, those are:

- Loss of user data due to accident or deliberate intrusion is known as a data breach.
- Traffic Hijacking on an Account or Service might cause the loss of financial control for the victim. The attacker gains access to mission-critical components of the service in production.
- One of the most problematic cases is a Denial of Service (DoS), which occurs when cloud resources are unavailable. DoS attacks in the Cloud are even more severe than their on-premises counterparts.
- The danger posed by malicious insiders is becoming a significant concern in the Cloud. The risk is that a dishonest insider, such as an employee, may attempt to get unauthorized access to private data.

Even though Cloud has become a significant business avenue for the present day, security concerns for Cloud are on the rise. More than a billion Chinese residents' personal information was recently stolen from a Shanghai police database, and the hackers who did it attempted to blackmail the police force for over $200,000. The database was hosted by Alibaba Cloud, a division of the Chinese e-commerce giant Alibaba, and the data was stolen from there [7]. Al Awadhi et al. [8] have provided evidence of the dangers to which the Cloud is vulnerable. Using honey-pots, they verified that the cloud environment is susceptible to assaults from various nations. Bellare et al. [8] presented a new cryptographic primitive called Message Locked encryption (MLE). The message serves as the key for both the encryption and decryption processes.

Khan et al. [9] presented Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) encryption as a means of protecting cloud-stored information. Compared to RSA, ECC's smaller critical sizes result in lower computing costs. However, ECC decryption time is longer than RSA. Further exploration is needed to optimize ECC's decryption time and evaluate its suitability for cloud environments. To counter the weakness of the original Multiple Huffman Tables (MHT) against selected plaintext attacks, Dahua Xie and Jay Kuo [10] suggested an improved encryption method using MHT with key hopping (CPA). This improved MHT encryption technique addresses the shortcomings of the earlier technology.

Using AES encryption and a third-party auditor for user verification and selection, K M Anil et al. [11] suggested a cloud server security paradigm to protect user data. The model ensures data authenticity and protection from intruders through encryption. The user receives the encrypted data upon request and decrypts it locally. Combining the strengths of AES and Blowfish, a hybrid encryption method was presented by Ali E. et al. [3]. The algorithm is designed for specific applications such as banking, military, big websites with extensive databases, and network companies. Using statistical tests to assess their effectiveness, the author evaluated various encryption algorithms, including AES, DES, Blowfish, and RSA. Kuzminykh et al. [13] have described The SWOT analysis. It estimates Knowledge Management Systems (KMSs) based on various attributes. Internal attributes include features, performance, storage, audit log, access control, authentication, documentation, HSM support, commercial use, usability, and installation. External attributes include security vulnerabilities, open issues ratio, active development, technical support, popularity, unit tests, and extendability.

3. Proposed System

This section presents our comprehensive and innovative system designed to deliver optimized and secure services in a cloud environment. With the ever-increasing reliance on cloud computing and the simultaneous rise in cyber threats, it has become imperative to develop robust solutions to safeguard sensitive data while ensuring efficient service delivery. Our proposed system addresses these challenges by integrating advanced encryption mechanisms, intelligent load-balancing techniques, and robust content delivery networks into its architecture. The primary objective is establishing a secure and optimized environment that protects data transmission and enhances overall system performance.

At the core of our system lies the utilization of Enhanced AES encryption, a state-of-the-art encryption algorithm. By leveraging critical scheduling, a Substitution-Permutation network, and hardware acceleration, we enhance the security of data travelling to and from the Cloud. This encryption system can guarantee that private data stays private by protecting data from prying eyes. Our system also uses hashing techniques, such as SHA256, to ensure the security of your data. These algorithms generate unique hash values for each file, enabling efficient data storage by eliminating redundancies. By avoiding the repetition of identical files, our system optimizes storage capacity, reduces network bandwidth usage, and improves data retrieval times.Our proposed system incorporates intelligent load-balancing techniques to enhance the overall system performance further. These techniques distribute incoming traffic across multiple servers and resources in a balanced manner, preventing overload on any single component. Caching mechanisms store frequently accessed data closer to the users, minimizing latency and response times. Content delivery networks (CDNs) are employed to optimize content distribution, ensuring that data is delivered from the nearest and most efficient server location. Our proposed system's combination of robust encryption, intelligent load balancing, and content delivery networks contributes to establishing a secure and optimized cloud environment. By addressing both the security and efficiency aspects, our system aims to meet the growing demands of organizations and individuals relying on cloud services.

The following sections will provide detailed insights into each component of our system, showcasing their functionalities, benefits, and contributions to the overall system architecture. The following are the advantages of the Proposed System,

- Enhanced Security
- Efficient Resource Utilization
- Improved System Performance
- Cost-effectiveness
- Scalability and Flexibility
- Reduced Downtime and Improved Reliability
- Compliance and Regulatory Requirements

A. System Architecture

In Figure 1, we see the overall system layout. There are four levels to this model.

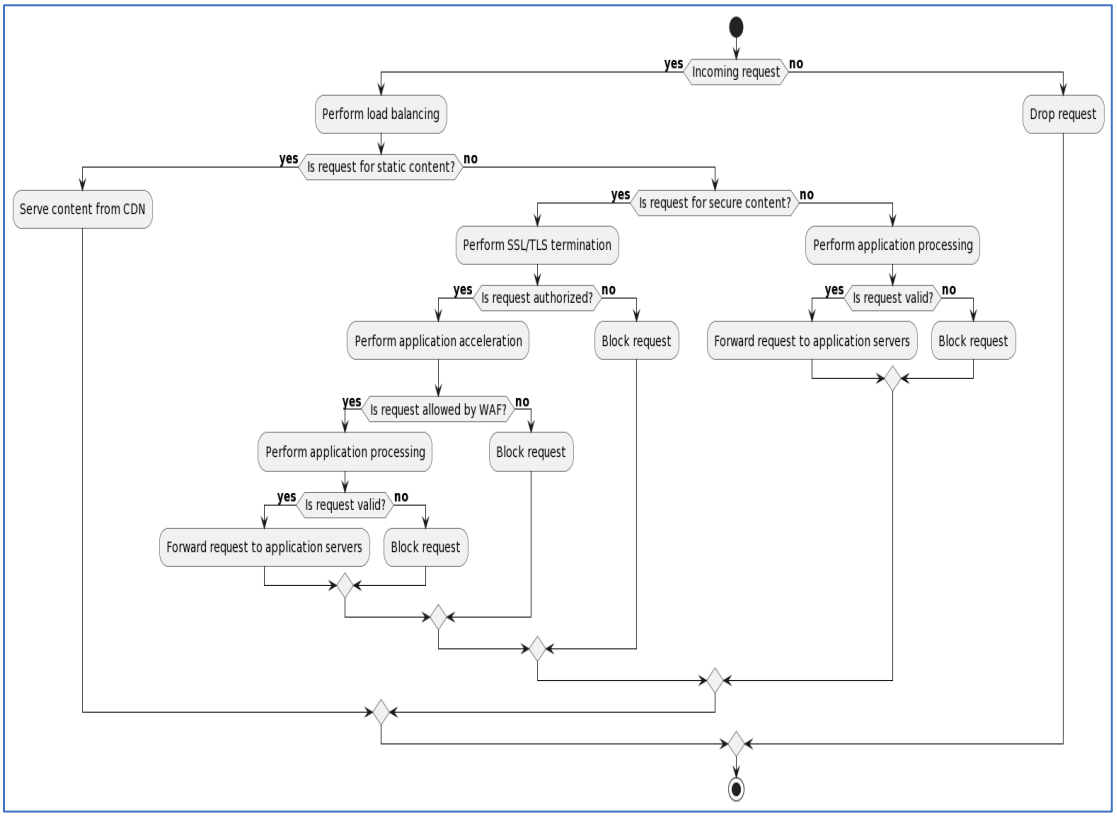

Fig. 1. Model Architecture Illustration

a) Cloud Environment:

As a cloud-based solution, the suggested system uses IaaS, PaaS, and SaaS paradigms to provide the necessary services. The Cloud's scalability and adaptability give users on-demand access to various computer resources, programs, and services. However, ensuring data security is crucial due to the increasing risks in the Cloud. The system focuses on securing data transmission, employing encryption mechanisms and optimizing service delivery through load balancing, caching, and content delivery networks.

b) Application Delivery Service Layer:

The application layer of the proposed system focuses on optimizing and securing service delivery within the cloud environment. It incorporates load balancing techniques to efficiently distribute traffic and caching mechanisms to store frequently accessed data, improving system performance. Content Delivery Networks (CDNs) are utilized for faster and more reliable content delivery by replicating data across geographically distributed servers. Enhanced AES encryption ensures secure transmission of data, protecting against unauthorized access. By combining these components, the application layer aims to provide optimized and safe service delivery, improving performance, reducing latency, and safeguarding sensitive data in the Cloud.

c) Cloud Service Provider (CSP):

The cloud service provider is a critical component of the proposed system, offering scalable and flexible cloud infrastructure. They manage hardware, networking, and virtualization technologies, ensuring high availability and performance. Users can focus on their core operations while leveraging the cost-efficiency and scalability of cloud computing. The cloud service provider offers different models, such as IaaS, PaaS, and SaaS, enabling businesses to access and deploy applications seamlessly.

d) User/Application Layer:

The user application layer facilitates user interaction with the Cloud, enabling easy access to services and applications. It offers a user-friendly interface for resource management, application deployment, and data processing. Users can seamlessly store, retrieve, and manipulate data, customizing their cloud experience. This layer streamlines user operations and empowers them to leverage cloud computing benefits effortlessly.

4. Components of Application Delivery Service Layer

The components of the application delivery service layer in the proposed system include:

Load Balancer: This component splits incoming network traffic among many servers for optimal resource usage and load balancing. It uses round-robin, least-connections, or weighted distribution methods for optimum load balancing.

Content Delivery Network (CDN): A content delivery network (CDN) is an international system of servers. Static resources (including photos, videos, and documents) are stored on the server nearest the user and served up quickly. It speeds up content transmission while reducing delays.

Web Application Firewall (WAF): Web application firewalls (WAFs) defend against DDoS, XSS, and SQL injection threats, among others, to keep websites running smoothly. It analyzes incoming data and filters out unwanted requests while letting valid ones through.

Application Acceleration: This component employs techniques like caching, compression, and protocol optimization to improve the performance of web applications. Caching stores frequently accessed data closer to the user, reducing the load on the backend servers. Compression reduces the size of data transferred, optimizing bandwidth usage. Protocol optimization enhances network communication efficiency.

SSL/TLS Termination: This component handles SSL/TLS encryption and decryption, removing the processing burden from backend servers. It provides secure communication between clients and servers by establishing secure connections and managing cryptographic operations.

Application Firewall: An application firewall protects web applications from application-level attacks, such as code injection and session hijacking. It analyzes application traffic, identifies negative behaviour patterns, and blocks suspicious requests. Application Delivery Controller (ADC): The ADC is a centralized control point for managing and optimizing application delivery. It performs functions like traffic management, SSL offloading, session persistence, and health monitoring of servers. It ensures high availability, scalability, and reliability of applications. These components work together to optimize application delivery, improve performance, enhance security, and provide an efficient user experience in the cloud environment.

Table 1. Comparison between Enhanced AES and different Algorithms

Algorithm	**Key Length**	**Block Size**	**Mode of Operation**	**Strength**	**Speed**	**Usage**
Enhanced AES	128-256 bits	128 bits	CBC, CTR, GCM	High	Moderate	General-purpose
RSA	1024-4096	Not applicable	Not applicable	High	Slow	Key exchange, digital signatures
Blowfish	32—448 bits	64 bits	CBC, CTR ,ECB	Medium	Fast	Legacy systems, file encryption
3DES	168 bits	64 bits	CBC, ECB	Low	Slow	Legacy systems

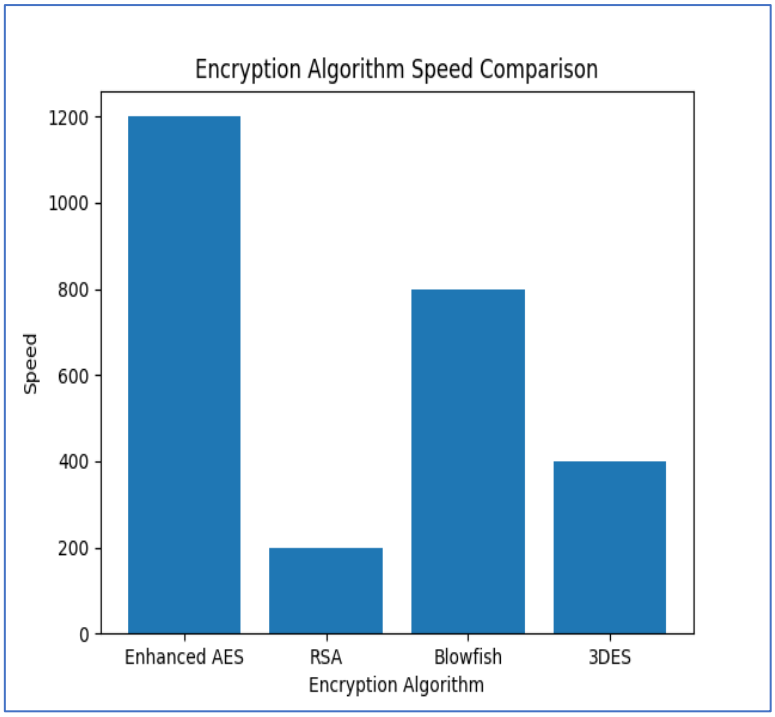

Fig. 2. Speed comparison between encryption algorithms.

5. Conclusion

In conclusion, the proposed model for application delivery service with optimization and enhanced security in the cloud environment addresses the crucial challenges of data security and efficient service delivery. We create a secure and optimized system by integrating advanced encryption mechanisms, intelligent load-balancing techniques, and content delivery networks. The safety and privacy of information sent to and from the Cloud are protected by enhanced AES encryption. Hashing algorithms like SHA256 prevent redundancies and optimize storage capacity, reducing network bandwidth usage. Intelligent load-balancing techniques distribute traffic across multiple servers, preventing overload and improving overall system performance. Content delivery networks (CDNs) minimize latency by delivering content from the nearest and most efficient server location. Combining robust encryption, intelligent load balancing, and CDNs establishes a secure and optimized cloud environment. This model offers enhanced security, efficient resource utilization, improved system performance, cost-effectiveness, scalability, and flexibility. By meeting the growing demands of organizations and individuals relying on cloud services, our proposed system contributes to advancing cloud computing technology.

References

[1] Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.

[2] Malik, Mohammad Ilyas. (2018). CLOUD COMPUTING-TECHNOLOGIES. International Journal of Advanced Research in Computer Science. 9. 379-384. 10.26483/ijarcs.v9i2.5760.

[3] Cyber Attacks on Cloud Services Rise 630% - Compliancy Group (compliancy-group.com)

[4] Gupta H, Sahu K (2014) Honey bee behavior based load balancing of tasks in cloud computing. Int J Sci Res 3(6

[5] C. Papagianni, A. Leivadeas and S. Papavassiliou, “A Cloud-Oriented Content Delivery Network Paradigm: Modeling and Assessment,” in IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 5, pp. 287-300, Sept.-Oct. 2013, doi: 10.1109/TDSC.2013.12.

[6] Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. Comput. Electr. Eng., 59, 126-140.

[7]https://www.immuniweb.com/blog/top-10-cloud-security-incidents-in-2022.html

[8] E. A. Awadhi, K. Salah and T. Martin, “Assessing the security of the cloud environment,” 2013 7th IEEE GCC Conference and Exhibition (GCC), Doha, Qatar, 2013, pp. 251-256, doi: 10.1109/IEEEGCC.2013.6705785.

[8]Bellare, M., Keelveedhi, S., Ristenpart, T. (2013). Message-Locked Encryption and Secure Deduplication. In: Johansson, T., Nguyen, P.Q. (eds) Advances in Cryptology – EUROCRYPT 2013

[9] I.A. Khan and R.Q. Qazi, "Data Security in Cloud Computing Using Elliptic Curve Cryptography", International Journal of Computing and Communication Networks, vol. 1, no. 1, pp. 46-52, 2019.

[10] Dahua Xie and C.-C. Jay Kuo, "Enhanced multiple Huffman table (mht) encryption scheme using key hopping" IEEE Transactions pp. 568- 571,2004

[11] K. M. Akhil, M. P. Kumar and B. R. Pushpa, "Enhanced cloud data security using AES algorithm," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 2017, pp. 1-5, doi: 10.1109/I2C2.2017.8321820.

[12] Ali E. Taki El_Deen, "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, vol. 4, no. 12, pp. 669-673, December 2013

[13] I. Kuzminykh, M. Yevdokymenko and D. Ageyev, "Analysis of Encryption Key Management Systems: Strengths, Weaknesses, Opportunities, Threats," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 515-520, doi: 10.1109/PICST51311.2020.9467909.

[14] Rihan, Dominic & Salih, Ahmed & Eldin, Saife & Osman, Faten. (2017). A Performance Comparison of Encryption Algorithms AES and DES. International Journal of Engineering Research.