International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Model of Access Control for Cloud Computing using Key Generation Based Public Cyclic Key Generation Method

Ranjeet Osari*[1], Rahul Singhai[2]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract:Cloud computing is a big platform of service-oriented applications over the internet. The primary access control of cloud services using login credentials for users. The growing rate of malicious software breaks the security credentials of users and theft data, and blocks the services. To prevent security threats, cloud service providers and NIST design various access control using cryptography algorithms. However, the role-based access control mechanism has limitations and breaks the security bridge between users and service providers. This paper proposed key generation-based access control methods for accessing services and data over cloud computing. The proposed key generation approach is a public key generation algorithm, a cyclic key generation algorithm. The proposed key generation methods are implemented in the Java RMI model and MYSQL database. The proposed algorithm compares with RSA based key authentication approach. The experimental results suggest that the proposed algorithm is better than the existing algorithm of access control of cloud computing.

Keywords:Cloud Computing, Access Control, Authentication, RSA, Public Key, RMI.

1. Introduction

Cloud computing represents a paradigm shift in how computing services are delivered and utilized over the Internet, encompassing a range of services categorized into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). [1] These services offer on-demand and scalable resources to users and organizations, significantly enhancing the accessibility of data processing, CPU processing, and storage management capabilities globally. [2] The adoption of cloud computing has led to a notable increase in the utility of these computing models for a diverse user base .

Despite the myriad benefits, the adoption of cloud computing is continually challenged by security threats, which undermine the integrity and authentication of user data and services. Security concerns are identified as a primary barrier to the broader acceptance of cloud computing, with threats including malicious code, back doors, Man-in-the-Middle (MitM) attacks, Distributed Denial of Service (DDoS) attacks, vulnerable application programming interfaces (APIs), exploitation of cloud resources, and various loopholes potentially compromising cloud services . [3] These security vulnerabilities can render cloud services inaccessible, adversely affecting their availability and reliability. Ensuring the continuous usability and availability of cloud services is, therefore, a critical obligation for cloud service providers .

Additionally, cloud computing introduces unique concerns related to the relocation and storage of resources and data in potentially diverse jurisdictions, each with its own regulatory frameworks and compliance requirements . While existing access control models could be adapted for cloud environments, this approach may not sufficiently address the complex security challenges of cloud computing, potentially overlooking multifaceted issues in favor of focusing on single-issue solutions within specific platforms or contexts . [4] The absence of comprehensive access control standards specifically tailored for cloud computing highlights the necessity for a detailed understanding and analysis of the extensive list of requirements critical for the success of any cloud computing access control system .

The increasing sophistication of attackers aiming to exploit cloud security vulnerabilities further accelerates the risk of data leakage to cloud services. Consequently, engineers and researchers are actively engaged in identifying potential threats and developing robust security models to protect sensitive data and cloud environments. [5] Recent proposals for secure data models in cloud computing emphasize the importance of

[1] *Research Scholar,Department of Computer Science, SCSIT , Devi Ahilya Vishwavidyalaya, Indore , M.P. , India*
[2] *Research Supervisor,Department of Computer Science, IIPS , Devi Ahilya University, Indore , M.P. , India*
Email :ranjeet.osari@gmail.com , singhai_rahul@hotmail.com
** Corresponding Author Email: ranjeet.osari@gmail.com*

addressing privacy concerns associated with transferring data to off-site storage solutions managed by third-party service providers. Issues such as the unauthorized disclosure of sensitive information, data integrity, and authenticity are of paramount concern .

In addressing the confidentiality of exchanged information, encryption before cloud storage emerges as a common strategy. Customers may encrypt their files using public key infrastructure and store them on cloud servers, with decryption keys shared only with authorized users . While this method enhances confidentiality, [6] it requires sophisticated control and distribution mechanisms to remain effective, especially as the user base expands . Cryptography, including the generation of public and private keys through algorithms such as RSA, AES, DES, and others, plays a crucial role in the authentication and security of cloud-based services, underscoring the ongoing need for advanced cryptographic solutions in cloud computing security [7].
This paper proposed cyclic key generation methods for the authentication of access control for the submission and retrieval of user's data. the rest of paper organized as in section II related work, in section III proposed Methodology, in section IV experimental analysis and finally conclude in section V.

II. Related Work

The security of access control within cloud computing represents a significant challenge amidst the evolving landscape of the internet. Various models have been proposed by researchers to enhance the security of cloud data storage and retrieval. Among these, the incremental model and algorithm development approach have been highlighted for strengthening cloud computing security.
A study introduced a honeypot-based access control model addressing authentication, logging, and other parameters by creating honeypots to trap unauthorized users, indicating the complexities surrounding data security in the cloud [1]. Another research outlined a unified cloud access control paradigm, leveraging centralized management across multiple Cloud Service Providers (CSPs) and employing role-based access control to enforce the principle of least privilege . Further, an efficient revocable attribute-based encryption technique has been proposed, offering a viable solution for attribute-based access control in IoT cloud environments, efficiently handling key revocation and decryption [2] .
Moreover, SEAPP, a secure application management system, was developed to protect against malicious attacks by managing application permissions and encrypting REST API requests, demonstrating low CPU and memory overheads alongside enhanced security [3].
In the realm of Industrial Internet of Things (IIoT), a cloud-assisted secure data access control system was introduced, employing ciphertext policy-attribute based encryption (CP-ABE) to achieve fine-grained access control and item-level data protection, thus addressing key leaking issues [4] .
Lastly, the examination of access control models and policies across various network settings and application scenarios, especially in cloud computing, reveals the connection between models, technologies, and their application benefits and drawbacks [5]. This overview also highlights the evolving challenges in access control and suggests future research directions within cloud computing [6].
The discourse on cloud computing security has expanded into various innovative approaches to ensure safe data sharing and robust access control mechanisms across multiple domains. For instance:
Researchers have developed a system for the flexible sharing of encrypted data among selected users, allowing for on-demand access control. This method enables users to decrypt data if their attributes align with the specified access policy and they possess a compact key for the required ciphertext classes, thereby promoting secure and efficient data sharing within cloud environments [7] .
Another study introduces an access control model that leverages a privacy rating (PR)-based strategy to safeguard health data. By evaluating the privacy ratings of both users and data, the model ensures high levels of privacy, confidentiality, and availability, addressing critical needs in healthcare data security [8].
A novel approach utilizes a dynamic revocable three-factor mutual authentication key agreement (MAKA) protocol based on Schnorr signatures. This protocol supports dynamic user management and provides formal security validation, making it highly suitable for smart devices with limited computational resources. It demonstrates the protocol's practicality in multi-server environments through extensive simulation [9] .

Discussion on the implementation of statistical analysis methods for data encryption and decryption, specifically focusing on Format-Preserving Encryption (FPE) and FF1 algorithms. The goal is to streamline access control by enabling selective encryption and secure data sharing through client-side key distribution and access control lists, thus eliminating the need for administrative interventions for key redistribution or data re-encryption when modifying access rights or managing users [10] .
The landscape of data security and access control continues to evolve with innovative research contributing to more sophisticated and efficient solutions. Here's a summary of recent advancements:
A novel approach integrating fuzzy logic and ontologies

for dynamic access control, leveraging contextual information to define access policies. This method demonstrates efficient query response times, underscoring its practical viability for managing access to data and information resources based on contextual conditions [11] .

Modifications to the Hierarchical Attribute-Based Encryption (HABE) model using the H-KCABE technique have shown improvements in performance, particularly through an optimized re-encryption process, facilitating more granular access control of cloud data [12] .

In the realm of fog computing, the SAKA-FC system offers a secure and efficient solution for key management and user authentication, proving its effectiveness even on resource-constrained devices through comprehensive security analyses and simulations [13].

The study examines the application of various attribute-based encryption methods to ensure the privacy and security of patient data in cloud healthcare systems, highlighting the challenges in protecting sensitive health information [14] .

A hybrid encryption framework that combines symmetric and asymmetric encryption techniques for secure data sharing, featuring a well-designed key management system. The Out FS file system shows promising results in protecting data integrity and resisting common security threats [15].

Decentralized Secure Communication in Vehicular Edge Computing: Research into a decentralized attribute-based encryption (ABE) scheme tailored for vehicular edge computing applications offers a novel method for flexible data encryption and access control, facilitating secure and efficient communication in automotive networks without the need for a predetermined secure channel [16] .

Addressing the challenges of user revocation and secure access, this approach introduces a dynamic, multi-authority access control mechanism for cloud data, which not only supports fine-grained access control but also ensures the system's security and efficiency through rigorous analysis and simulations [17] .

The exploration of data protection techniques in the digital realm, particularly in cloud computing, has led to significant research advancements in integrity, accountability, privacy, access control, authentication, and authorization. Among these developments, blockchain technology emerges as a promising solution to enhance security in cloud computing, addressing various security challenges inherent to the cloud environment. This research survey compares and contrasts issues related to cloud computing and blockchain security, shedding light on how blockchain can mitigate cloud computing security concerns [18] .

Furthermore, the AKM-IOV method is introduced as a secure and authenticated key management process tailored for fog computing-based Internet of Vehicles (IOV) applications. The AKM-IOV's security credentials are validated through rigorous analysis under the "Real-Or-Random (ROR)" model and both casual and formal security verification using the "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool. Practical applicability is demonstrated via NS2 simulations, and a comprehensive comparative analysis underscores AKM-IOV's superior efficiency, functionality, and security over existing protocols [19] .

Additionally, an innovative Encryption Access Control (EAC) system is discussed, which effectively addresses both attribute and user revocation challenges. By uniquely generating a secret token key for each classification level and subsequently hashing this token to produce a new secret key, the system ensures secure policy revocation. The research compares key generation, encryption, and decryption times between scenarios with and without policy revocation, providing a detailed performance analysis of the policy revocation process [20] .

3. Proposed Methodology

This section describes the proposed methodology of secure access control of user's data over the internet. First, the server derives the session key generation between users and the cloud server to share and retrieve data over the cloud. The generation of crucial uses public cyclic key methods. The public cyclic key generation method is focused on the circle point of data [19]. The previous estimation of the key expires after the second stage of key formation generation. The description of models as consider X1 key used by the user and X2 key used by the cloud server, K is cyclic intermediate key S1 and S2 is side of user and server.

Algorithm:

The generation of cyclic key uses three factors S1, S2 and K

CK = V {S1, S2, K}

The cyclic key form a round of radix of cyclic value

Value1 = round mod(k-3)

Value 2= round mod(k-2)

Value3 = round mod(k-1)

The formation of hash value of generated key as

hash = h{Value1,Value2,Value3}

session of key between cloud service provider and users as

SK1={S1, hash, S2}

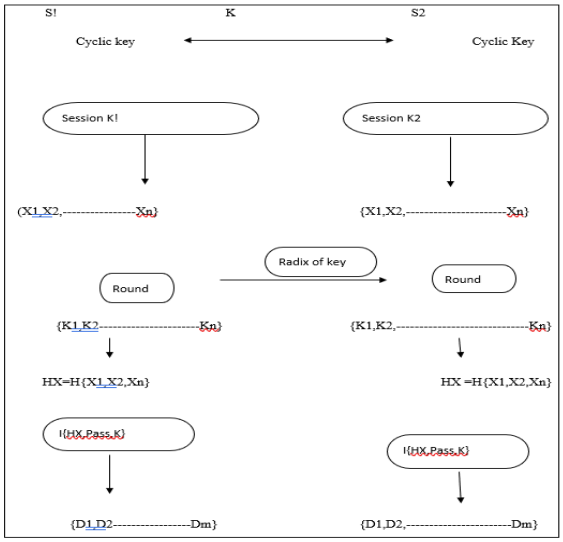


Figure 1 process block diagram of key generation between user and cloud service provider

4. Experimental Analysis

To validate the proposed access control methods using cyclic key generation implements in java language with MYSQL database. For the implementation of java use NetBeans 8.2 software, the main tools of Java is RMI control to design server side and users side. The system configuration I7 processor, 16GB ram and windows operating system [20]. The performance of algorithm estimated with two parameters hit and miss ratio of cloud files. The implementation scenario shown in figure 2 below.

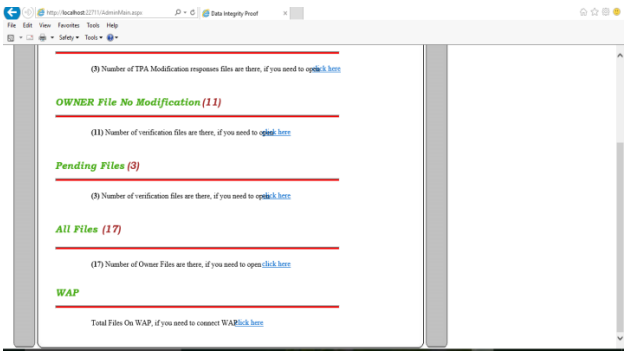


Figure 2 shows the processing of file system in implementation scenario as source file, pending file, WAP file

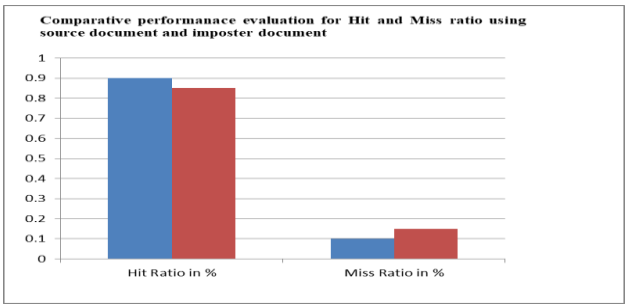
Table 1: Demonstrates the difference in performance between the real and phoney files based on the percentage value of the hit and miss ratio for the hello and jaipur files.

Data	Name of data	Hit Ratio in %	Miss Ratio in %	Flag value
Source document	Hello.txt	0.9	0.1	False
Imposter document	jaipur.txt	0.85	0.15	True

Table 2: Demonstrates the difference in performance between the real and phoney files based on the percentage value of the hit and miss ratio for the ram and sita files.

Data	Name of data	Hit Ratio in %	Miss Ratio in %	Flag value
Source document	ram.txt	0.88	0.12	False
Imposter document	Sita .txt	0.81	0.19	True

Figure 3: Demonstrates the graph of comparative performance evaluation between the source and impostor files, based on the percentage value of the hit and miss ratio for the hello and Jaipur files.



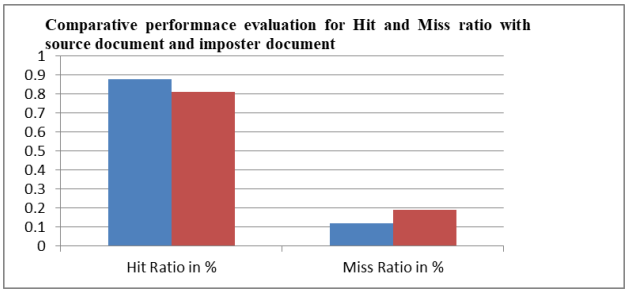


Figure 4: Demonstrates the graph of comparative performance evaluation for source and impostor files based on the percentage value of the hit and miss ratio for the ram and sita files.

Table 3: Demonstrates the relative effectiveness of the RSA Based, Cyclic Based, and DRDP Based computation times based on block size.

DRDP Method		RSA Based instantiation		Cyclic Based	
Block Data size	Computation Time	Block Data size	Computation Time	Block Data size	Computation Time
0	200	0	220	0	210
20	220	20	240	20	230
40	240	40	260	40	250
60	260	60	280	60	270
80	280	80	300	80	290
100	300	100	320	100	310
120	320	120	340	120	330
140	340	140	360	140	350
160	360	160	380	160	370
180	380	180	400	180	390

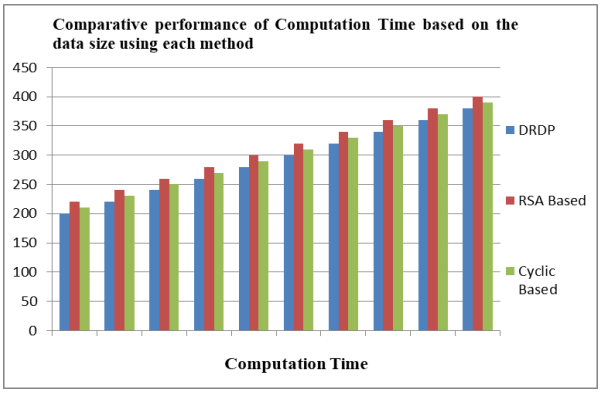


Figure 5: Demonstrates the relative performance for computation time based on data block size utilising various methods, such as RSA Based, Cyclic Based, and DRDP Based. Here, we discover the computation time value for the corresponding block size and methods.

5. Conclusion & Future Work

This paper proposes a secured access control method based on cyclic key generation. The proposed methods generate key values to authenticate users and cloud service providers. The formation of the key is based on the concept of a circle, so the previous value of the key is lost after the generation of the second value of the key. The proposed methods apply three factors: server-side, user side, and cyclic K. The key session is decisive instead of previous key generation methods. The proposed method tested on different files as the source document and imposter document, and the false value of the file is true, false. The analysis of results suggests that the proposed algorithm is very efficient instead of existing algorithms such as DPRM, RSA. From the standpoint of this work, we intend to implement verification and authentication mechanism capable to dealing with time complexity and space complexity. We will also put in place the risk engine and its components to deal with erratic behavior. This model will be put into action after the authentication has been implemented, evaluated mechanism and risk generator.

Acknowledgments

Ranjeet Osari: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Validation. **Rahul Singhai:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1]. Khashan, Osama Ahmed. "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System." *IEEE Access* 8 (2020): 210855-210867.

[2]. Sukmana, Muhammad IH, Kennedy A. Torkura, Hendrik Graupner, Feng Cheng, and Christoph Meinel. "Unified cloud access control model for cloud storage broker." In *2019 International Conference on Information Networking (ICOIN)*, pp. 60-65. IEEE, 2019.

[3]. Xu, Shengmin, Guomin Yang, Yi Mu, and Ximeng Liu. "A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance." *Future Generation Computer Systems* 97 (2019): 284-294.

[4]. Hu, Tao, Zhen Zhang, Peng Yi, Dong Liang, Ziyong Li, Quan Ren, Yuxiang Hu, and Julong Lan. "SEAPP: A secure application management framework based on REST API access control in SDN-enabled cloud environment." *Journal of Parallel and Distributed Computing* 147 (2021): 108-123.

[5]. Qi, Saiyu, Youshui Lu, Wei Wei, and Xiaofeng Chen. "Efficient data access control with fine-grained data protection in cloud-assisted IIoT." *IEEE Internet of Things Journal* 8, no. 4 (2020): 2886-2899.

[6]. Cai, Fangbo, Nafei Zhu, Jingsha He, Pengyu Mu, Wenxin Li, and Yi Yu. "Survey of access control models and technologies for cloud computing." *Cluster Computing* 22, no. 3 (2019): 6111-6122.

[7]. Sabitha, S., and M. S. Rajasree. "Multi-level on-demand access control for flexible data sharing in cloud." *Cluster Computing* 24, no. 2 (2021): 1455-1478.

[8]. Prince, P. Blessed, and SP JenoLovesum, "Privacy enforced access control model for secured data handling in cloud-based pervasive health care system." *SN Computer Science* 1, no. 5 (2020): 1-8.

[9]. Li, Wei, Li Xuelian, Juntao Gao, and Hai Yu Wang. "Design of secure authenticated key management protocol for cloud computing environments." *IEEE Transactions on Dependable and Secure Computing* (2019).

[10]. Inampudi, Govardhana Rao, KurraMalliah, and S. Ramachandram. "Key Management for protection of health care Data of Multi-user using Access control in Cloud Environment." In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, pp. 1-8. IEEE, 2019.

[11]. Kayes, A. S. M., Wenny Rahayu, Tharam Dillon, Elizabeth Chang, and Jun Han. "Context-aware access control with imprecise context characterization for cloud-based data resources." *Future Generation Computer Systems* 93 (2019): 237-255.

[12]. Sangeetha, M., P. Vijayakarthik, S. Dhanasekaran, and B. S. Murugan. "Fine grained access control using H-KCABE in cloud storage." *Materials Today: Proceedings* 37 (2021): 2735-2737.

[13]. Wazid, Mohammad, Ashok Kumar Das, Neeraj Kumar, and Athanasios V. Vasilakos. "Design of secure key management and user authentication scheme for fog computing services." *Future Generation Computer Systems* 91 (2019): 475-492.

[14]. Priyanka, J., and M. Ramakrishna. "Performance analysis of attribute based encryption and cloud health data security." In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 989-994. IEEE, 2020.

[15]. Khashan, Osama Ahmed. "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System." *IEEE Access* 8 (2020): 210855-210867.

[16]. Cheng, Cheng-Yu, Hang Liu, Li-Tse Hsieh, Edward Colbert, and Jin-Hee Cha. "Attribute-Based Access Control for Vehicular Edge Cloud Computing." In *2020 IEEE Cloud Summit*, pp. 18-24. IEEE, 2020.

[17]. Wang, Jian, Chunxiao Ye, and YangfeiOu. "Dynamic Data Access Control for Multi-Authority Cloud Storage." In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 599-608. IEEE, 2019.

[18]. Pavithra, S., S. Ramya, and Soma Prathibha. "A survey on cloud security issues and blockchain." In *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, pp. 136-140. IEEE, 2019.

[19]. Wazid, Mohammad, Palak Bagga, Ashok Kumar Das, Sachin Shetty, Joel JPC Rodrigues, and Youngho Park. "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of vehicles deployment." *IEEE Internet of Things Journal* 6, no. 5 (2019): 8804-8817.

[20]. Myint, Phyo Wah Wah, Swe Zin Hlaing, and Ei Chaw Htoon. "EAC: Encryption Access Control Scheme for Policy Revocation in Cloud Data." In *International Conference on Advanced Information Technologies (ICAIT)*, pp. 182-187. IEEE, 2020.