ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

SECURE MODEL OF ACCESS CONTROL FOR CLOUD COMPUTING USING KEY GENERATION BASED PUBLIC CYCLIC KEY GENERATION METHOD

Ranjeet Osari[1], Rahul Singhai[2]
[1] Department of Computer Science, SCSIT Devi Ahilya Vishwavidyalaya, Indore M.P. India
ranjeet.osari@gmail.com
[2] Department of Computer Science, IIPS Devi Ahilya University, Indore M.P. India
singhai_rahul@hotmail.com
Corresponding author: ranjeet.osari@gmail.com

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

I. Introduction

Cloud computing is a model of services and changes the ways of computing over the internet. The cloud Stack of services such as IAAS, PAAS, SAAS facilitates the users and organization. The delivery of services is based on demand and scalable on user and organization. The utility of cloud computing increases the number of users worldwide for data processing, CPU processing and storage management [1,2]. However, accessing data and services over cloud computing has always come under security threats. The security threats degrade the integrity and authentication of users. One of the primary concerns and a major impediment to cloud computing adoption is security [3]. Malicious code, back doors, Man-in-the-Middle attacks, Distributed Denial-Of-Service (DOS) attacks, insecure application programming interface, abuse and nefarious use of cloud computing, and malicious insiders are all potential security threats to cloud computing [4,5]. Cloud services may become inaccessible as a result of these attacks, having a negative impact. It is a critical requirement for cloud service providers to ensure that their services are fully usable and available at all times. Furthermore, cloud computing has raised new concerns, such as moving resources and storing data in the cloud, which may reside in another country with different regulations [6,7].Existing access control models may be able to be extended and used in the cloud environment. However, this could be a risk and may not solve the problem because traditional access models may focus on a specific problem in a specific platform or environment and overlook the remaining interconnected issues [8 ,9]. This could occur due to the lack of a comprehensive list of access control requirements for cloud computing. In other words, the

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

success of any cloud computing access control solution will be dependent on analyzing and accurately identifying a comprehensive list of requirements [10,11]. Data leakage to cloud services is also increasing year after year as a result of attackers who are constantly attempting to exploit cloud security vulnerabilities. Engineers and researchers attempt to identify potential cloud threats and attacks in order to better secure sensitive data and cloud computing environments [12]. Many data secure models for cloud computing have recently been propose. The cloud allows for open information sharing with others. Moving data to a third-party (cloud carrier provider) off-website online storage community over which information owners have little control poses distinct privacy issues (risks of illegal disclosure of sensitive information via carrier providers, facts integrity and authenticity of out-of-carrier information, and so on [13,14]. The cloud allows for the exchange of information; careful consideration should be paid to the complete get admission to manage of the saved information.is sensitive fact about confidentiality is a common method to encrypt it until its miles moved to the cloud computing. the customer encrypts his document and stores it in a traditional public key infrastructure on the cloud server, and the only genuine authorized consumer is informed about the decryption key [15,16]. This method is secure in terms of confidentiality; however, reliable, tested, and complicated control and distribution are required for this solution. Even this solution would fail because the number of software customers is increasing [17]. The cryptography plays a vital role in key generation and authentication of cloud-based services. The contribution of public and private key generation process such as RSA, AES, DES and many more derives algorithms of key generation [18].

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

Security of access control of cloud computing is a big challenge in the current scenario of the internet. For security access, various models are proposed by different authors and enhance the security of cloud data storage and retrieval. Moreover, the incremental model and algorithm development approach strengthen cloud computing security. Some current contribution of authors describes here. In this [1] researchers discussed the use of cloud computing has increased. With the adoption of cloud computing, many businesses are committing to storing and processing large amounts of data in the cloud. The facility providers' security measures may not be sufficient to protect data in the cloud. The right security aspect of storing, retrieving, and processing massive data in a cloud environment is causing problems for both enterprises and users. This study presents a honeypot-based access control model. The access control model deals with a variety of authentication, log, and other parameters. To catch hackers or unauthorized users, several links and areas are provided as honeypots. In this [2] researchers discussed the unified cloud access control paradigm abstracts CSP services to allow for centralized and automated cloud resource and access control management across many CSPs. Following the privilege separation idea and the least privilege principle, their solution provides role-based access control for CSB stakeholders to access cloud resources by providing necessary rights and an access control list for cloud resources and CSB stakeholders, respectively. their unified approach is implemented in a CSB system named Cloud RAID for Business, and the evaluation outcomes

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

demonstrate that it delivers system-and-cloud level security for CFB, as well as centralized resource and access control management in various CSPs. In this [3] researchers discussed an efficient revocable attribute-based encryption technique that allows the data owner to easily manage the credentials of data users, a viable attribute-based access control system for IoT cloud is created. Both secret key revocation for corrupted users and inadvertent decryption key exposure for honest users can be handled efficiently by their suggested method. they use formal proofs to assess the security of their scheme, and they use experiments to illustrate the discussed system's great performance. In this [4] researchers discussed SEAPP is a secure application management system based on access control using REST APIs. their main goal is to protect against malicious attacks by granularly managing application permissions and encrypting REST API requests. SEAPP is made up of two parts. The security and effectiveness of SEAPP are demonstrated by both theoretical analysis and evaluation outcomes. Furthermore, SEAPP has very low CPU and memory overheads. In this [5] researchers discussed the cloud- assisted IIOT'S safe industrial data access control system Participants can use their ciphertext policy-attribute based encryption (CP-ABE) technique to impose fine-grained access control policies for their IoT data. Importantly, their system ensures a novel privacy concept known as item-level data protection for IoT data, which prevents the problem of key leaking. Several encryption and optimization techniques are used to attain these objectives. their performance evaluations combine system implementation with large-scale emulations to ensure that their design is secure and efficient. In this [6] researchers discussed the growth of the internet as the main line and evaluating different network settings and user requirements, access control models and policies in various application scenarios, particularly for cloud computing the study focuses on the links between different models and technologies, as well as application scenarios and the benefits and drawbacks of each model. Access control for cloud computing will receive special attention, as evidenced by the overview of access control models and methodologies. they also identify some growing access control challenges and suggest some upcoming cloud computing research topics. In this [7] researchers discussed a flexible sharing of safe data among randomly selected users with on-demand access control It's a flexible sharing of ciphertext classes in the cloud with a customizable access control method. It only assigns users decryption rights for any collection of ciphertext classes if their attributes are compatible with the ciphertext access policy and if they have a compact key that corresponds to the desired set of ciphertext classes. In this [8] researchers discussed the suggested access control model, which uses a PR-based strategy for providing access control to various users of the system, provides strong privacy, data confidentiality, and availability against health data. The user's and the data's privacy ratings are determined in order to grant access to any data requested by the user. The obtained findings suggest that the discussed approach provides a high level of privacy and security for data held in the healthcare system. In this [9] researchers discussed the a provable dynamic revocable three-factor MAKA protocol that uses Schnarr signatures to accomplish user dynamic management and gives a formal security proof in the random oracle. their protocol can handle a variety of demands in multi-server systems, according to security study. The discussed system is highly suited for computational resource constrained smart devices, according to a performance analysis. The entire version of the simulation implementation demonstrates the protocol's viability. In this [10] researchers discussed the implementation and current performance of statistical analysis of approaches for

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

encrypting/decrypting data using FPE, FF1 with less computation and resource time, implementation of access control through selective encryption, providing secure access and sharing services for multi user's data using key distribution in the client side, and access control lists are discussed. The major purpose of this article is to eliminate the need for any administrative activities (such as modifying access privileges or adding/deleting users) to re-distribute keys or re-encrypt data. In this [11] researchers discussed the Fuzzy logic-based Context-Aware Access Control (FCAAC) for data and information resources. To capture the fuzzy and other contextual conditions, they offer a formal context model. they also present a formal policy model that uses these conditions to construct policies. they integrate the fuzzy model with an ontology-based approach that captures and incorporates such contextual circumstances into policies using ontology languages and fuzzy logic-based reasoning in their formal approach. Finally, they show how to perform an experimental evaluation of query response time. The outcomes of the experiments show that their discussed FCAAC technique performs well. In this [12] researchers discussed the H-KCABE encryption technique is used in the HABE model with some minor changes to improve performance through the re-encryption process. they can more easily achieve fine-grained access control of cloud data with this method than with previous techniques. In this [13] researchers discussed SAKA-FC is a novel secure key management and user authentication mechanism designed for fog computing environments. Because smart devices are resource-constrained, SAKA-FC is efficient because it only performs lightweight operations like one-way cryptographic hash function and bitwise exclusive-OR (XOR). The formal security analysis, which uses the widely accepted Real-Or-Random (ROR) model, the formal security verification, which uses the widely used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, and the informal security analysis all show that SAKA-FC is secure. SAKA-FC is also implemented for use with the widely used NS2 simulator for practical demonstration. In this [14] researchers discussed Cloud health care allows for quick and easy diagnosis, resulting in a more efficient situation in cloud health care. To make data easily accessible in all situations, patient information has been maintained in a single repository. One of the most significant drawbacks of using cloud health care data is the issue of security and privacy. This study examines the several types of attribute-based encryption. In this [15] researchers discussed a structure for a hybrid encryption technique based on symmetric and asymmetric methods The key management system is well-designed. The identity-based encryption system (IBE) is coupled with Out FS to ensure robust data sharing security. Out FS is a file system designed to protect the integrity of outsourced file data and the data structure of the file system. Out FS is efficient, according to performance analysis and experimental data. It has a throughput of 8.8 MB/sec on average, and 10.5 MB/sec when writing and reading outsourced files. Out FS is exceptionally safe and resistant against brute-force, eavesdropping, man-in-the-middle, and offline-dictionary attacks, according to security studies. In this [16] researchers discussed the development and testing of a secure communication scheme for vehicular edge computing applications based on decentralized attribute-based encryption (ABE), which allows for flexible data encryption and access control based on attribute-based policies without the need to know the recipient's identity or establish a secure communication channel between sender and recipient. For proof of concept, communication protocols are defined and an experimental prototype with an edge cloud-assisted collision warning application is implemented. The outcomes of the evaluation reveal that the

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

discussed ABE-based strategy is both efficient and practical. In this
[17] researchers discussed a fine-grained dynamic multi-authority cloud data access control approach that solves the two challenges mentioned above Furthermore, their system can support user revocation, making it more practical. The analysis and simulation outcomes show that their approach is both secure and efficient in the random oracle model. In this [18] researchers discussed Integrity, accountability, privacy, access control, authentication, and authorization are all critical data protection techniques that must be maintained. Blockchain is a technology that helps to improve cloud computing. Blockchain solves cloud computing's security problems. This survey intends to examine and compare various cloud-related issues as well as blockchain-related security concerns. In this [19] researchers discussed the AKM IOV is a secure authenticated key management protocol used in fog computing-based IOV deployment. The formal security analysis under the widely established "Real-Or-Random (ROR)" model, as well as informal and formal security verification utilizing the widely accepted "Automated Vali dation of Internet Security Protocols and Applications (AVISPA)" tool, are used to verify AKM-IOV. The NS2 simulation is used to demonstrate the practical application of AKM-IOV. A full comparative analysis is also carried out to demonstrate the efficiency, functionality, and security characteristics enabled by AKM-IOV when compared to other current protocols. In this [20] researchers discussed the to complete policy revocation, an encryption access control (EAC) system that encompasses both attribute and user revocation is used. Each secret token key is generated uniquely for each level by classifying those levels. As an outcome of hashing the secret token key, a new secret key is generated. The execution times of key generation, encryption, and decryption are compared between non-revocation and policy revocation instances in this work. This study also includes a performance analysis for policy revocation.

III. 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 sider of user and server.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

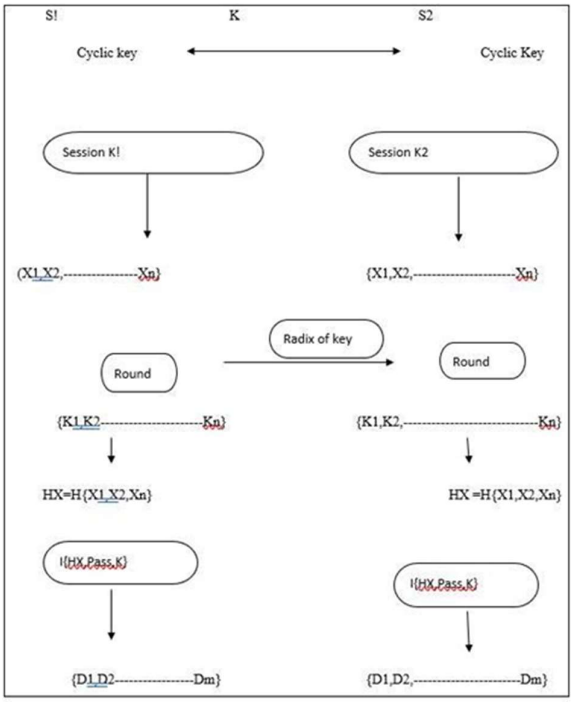

Figure 1 process block diagram of key generation between user and cloud service provider

Algorithm:

The generation of cyclic key uses three factors S1, S2 and KCK = 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}

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

IV. 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.

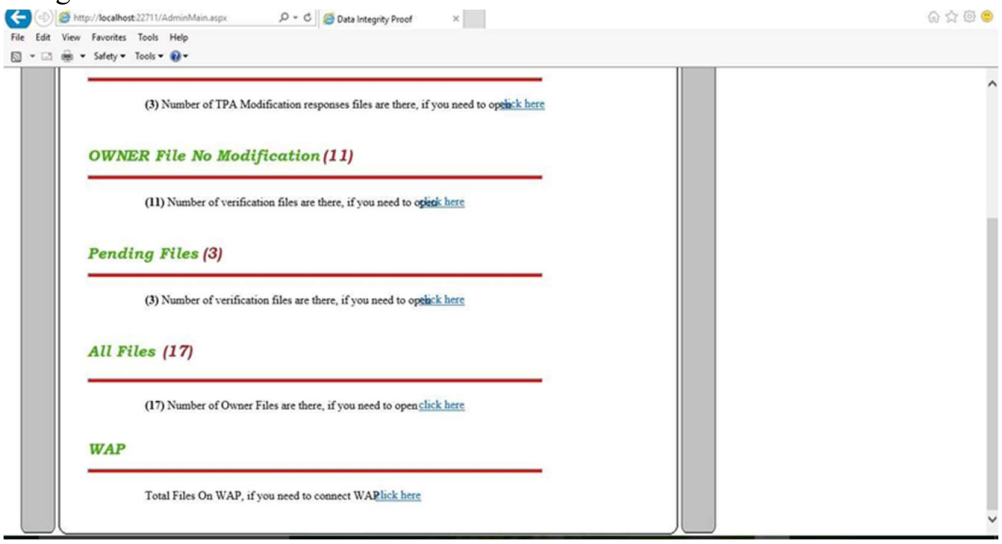

Figure 2 shows the processing of file system in implementation scenario as source file, pending file, WAP file

Table-1: Shows that the comparative performance for original and fake files based on number of hit and miss ratio in percentage value for the hello and Bca file.

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: Shows that the comparative performance for original and fake files based on number of hit and miss ratio in percentage value for the Aa and Ab file.

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

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

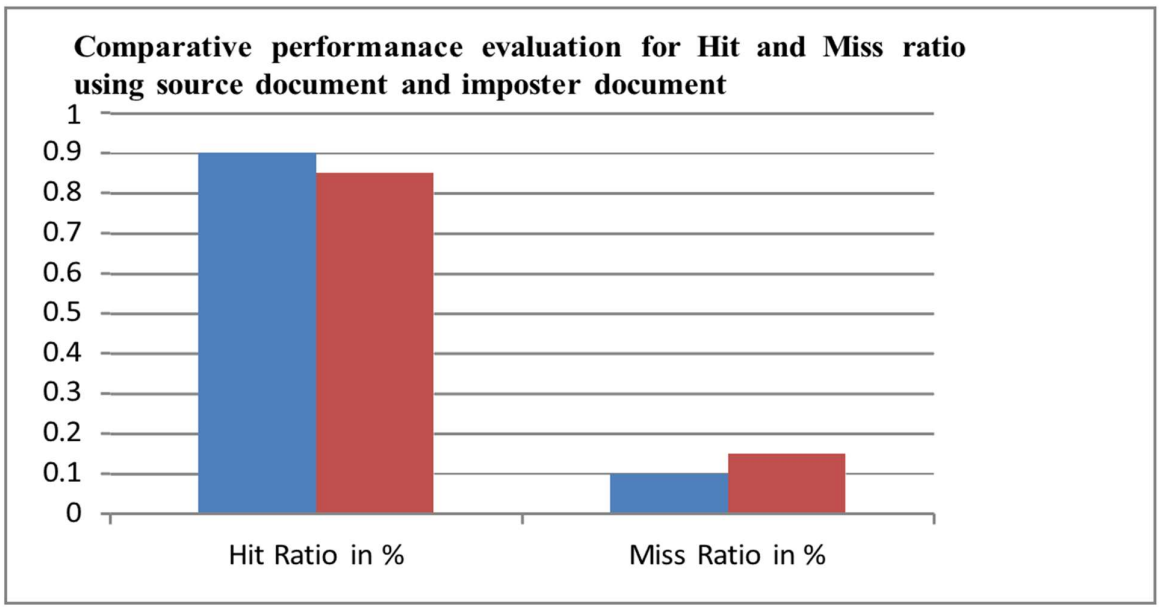

Figure 3: Shows that the comparative performance evaluation graph for source and imposter files based on number of hit and miss ratio in percentage value for the hello and Jaipur file.

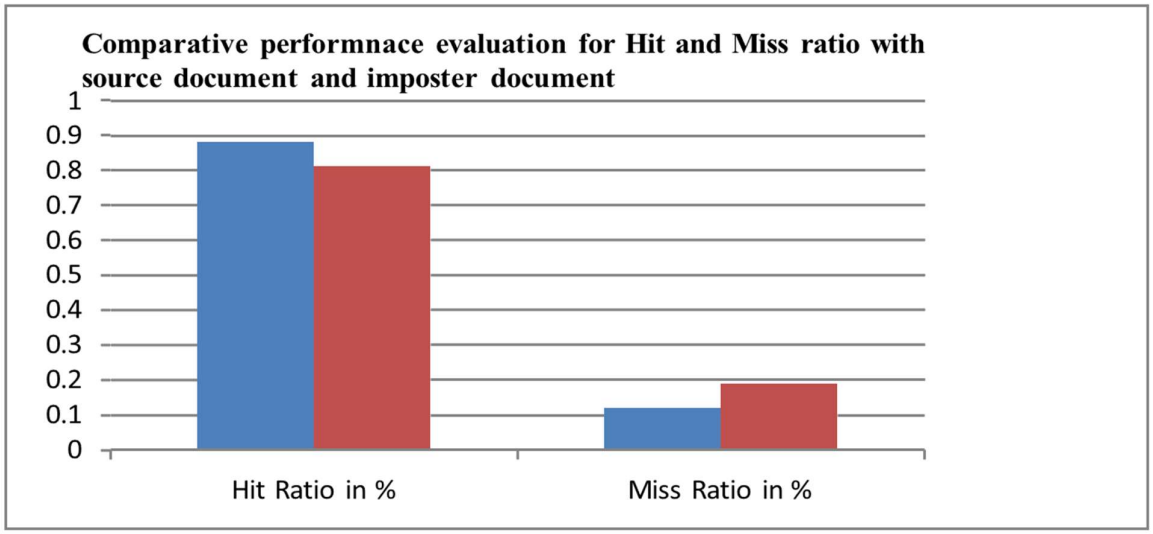

Figure 4: Shows that the comparative performance evaluation graph for source and imposter files based on number of hit and miss ratio in percentage value for the ram and sita file

Table-3: Shows that the comparative performance for Computation time on the basis of block size using methods DRDP, RSA Based and Cyclic Based

DRDP Method		RSA Based instantiation		Cyclic Based	
Block Data size	Computation Time	Block Data size	Computation Time	Block Data size	Computation Time

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

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

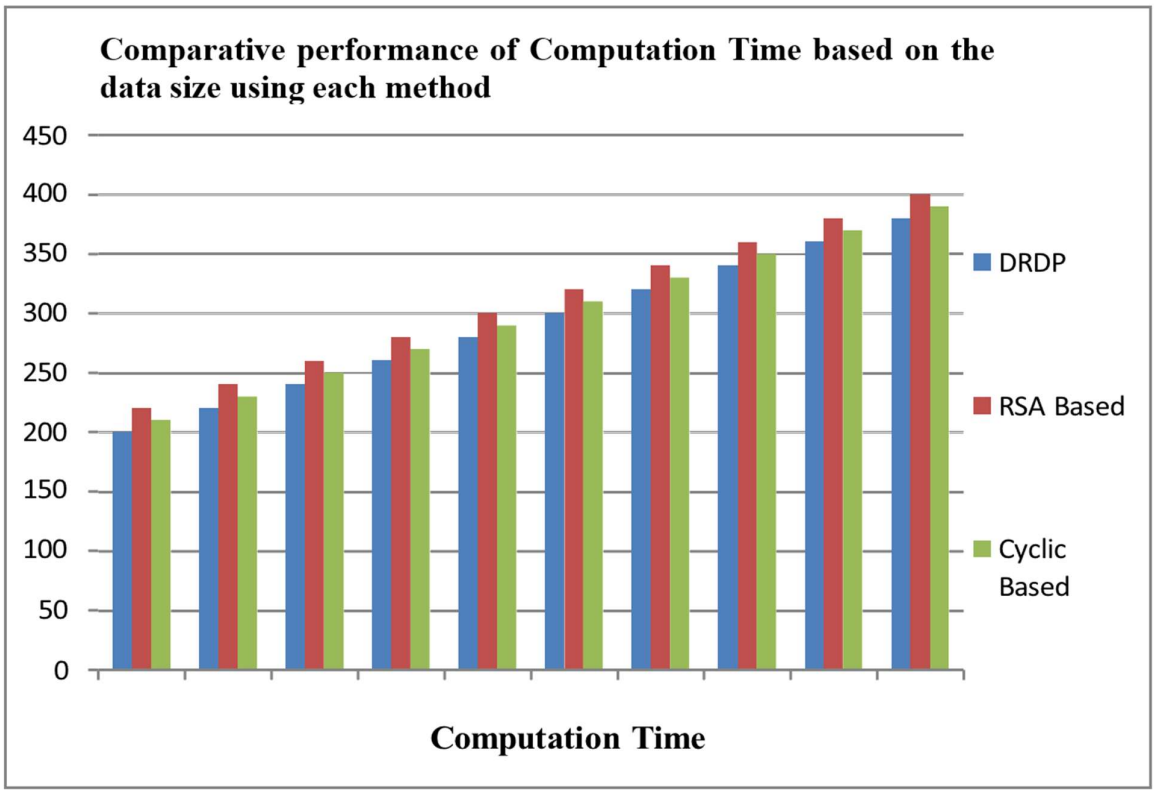

Figure 5 Shows that the comparative performance for Computation time on the basis of data block size using each method like DRDP, RSA Based and Cyclic Based, here we find the value of computation time for respectively block size and methods.

V. 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

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

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 an authentication mechanism capable of dealing with high time and space complexity. We will also put in place the risk engine and its components to deal with erratic behavior. The model will be put into action after the authentication has been implemented, evaluated mechanism and risk generator.

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-

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

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.
[21]. Monika Yadav and Manvi Breja. “Secure DNA and Morse code based Profile access control models for Cloud Computing Environment” In International Conference on Computational Intelligence and Data Science (ICCIDS 2020) Elsevier Science Direct Procedia Computer Science 167 (2020) 2590–2598.
[22]. Mohamad Mulham Belal and Divya Meena Sundaram “Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends” In Journal of King Saud University – Computer and Information Sciences Elsevier Science Direct 34 (2022) 9102– 9131.
[23]. Munwar Ali, Low Tang Jung, Ali Hassan Sodhro, Asif Ali Laghari, Samir Birahim Belhaouari and Zeeshan Gillani “A Confidentiality-based data Classification-as-aService (C2aaS) for cloud security” Alexandria Engineering Journal Elsevier 64 (2023), 749–760.
[24]. Seyed Farhad Aghili, Mahdi Sedaghat, Dave Singelée and Maanak Gupta “MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme” In Future Generation Computer Systems Elsevier Science Direct 131 (2022) 75–90.