International Journal of Engineering & Technology, 7 (1.1) (2018) 30-36

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Content arrangement characteristic based encryption in cloud using public auditing for data management

V. Joseph Michael Jerard[1*], P. Manimegalai [2]

[1]Research Scholar, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
[2]Professor, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
**Corresponding author E-mail:Jerard.vedam@gmail.com*

Abstract

The encryption standard related to cryptography provide the possible keys with logical standard for sharing and distributing sensitive information sharing worldview in conveyed frameworks. A Content Arrangement Characteristic Based Encryption (CA-CBE) is turning into a promising cryptographic solution for this issue. The cloud needs to provide the view on open auditability. Many methodologies have been discussed on dynamic information administration and on general auditability, however those methodologies suffer from the issue of check overhead and time multifaceted nature. Therefore, it is important to propose a Content Arrangement Characteristic Based Encryption (CA-CBE) scheme for supporting data dynamics over the data operation, like block alteration, block inset, and deletion. Some existing data integrity based research always lacks in dynamic operations and public auditability. By considering this as a motivation, this research is initiated.

Keywords: *Cloud, content arrangement characteristic based encryption, outsider auditing, cryptography*.

1. Introduction

In recent days, Cloud Computing based numerous developments are opening up with add-ons of internet and computer knowledge. It is quite complex to use the cloud computing for secure operational activities because it does not provide any alternative solution for this issues. Hence, there is a need for secure computing process. The ability to observe with any constraint is an immediate end result of its service and deployment process are employed. Improper usage of the data or unapproved access by unwanted people or customers could be potential hazards for those data. People may want to make their delicate or private information just available to the approved individuals with encrypted certifications.

Quality Based Encryption (QBE) is a talented cryptographic approach that provides and achieves fine-grained control on illustrating access approaches with various properties of the requester, the condition and information. Particularly, cipher text arrangement characteristic based encryption (CA-CBE) authorizes to encrypt or to characterize the quality over a set universe of properties and the decrypt have a specific end goal to decode the figure message, and uphold it on the substance.

In twofold encryption schemes, the keys and cipher texts are considered as one of two clear formats namely, normal and semi-functional. A standard key can decrypt both formats of cipher texts, whereas a semi-functional key has an ability to decrypt the normal cipher texts. In real time applications, semi-functional elements are rarely used. It is mostly utilized as a proof of security. Consequently, the significant advantage of this approach is to diminish the requirement for preparing and putting away open key declarations under conventional open key foundation. The upside of the CA-CBE accompanies a noteworthy disadvantage which is known as a key escrow issue. The attribute auditing can decode each cipher text routed to particular clients by producing their characteristic keys. This could be a potential risk to the information classification or security in the information sharing frameworks.

In the traditional CBE schemes, the probable values of each attribute is defined by the encryptor. The encryptor has a rights to control or hide some sort of possible values in cipher text for decrypting the data. Remaining part of this research is described as follows, section 2 provides detail literature review. Section 3 provides detailed representation of proposed encryption based methodology. Section 4 discusses outcome of this method. Finally, the article is summarized in section 5.

2. Literature survey

A. Reuter, Frederik Armknecht, et al, 2016 proposed Homomorphism encryption permits legitimate calculations straightforwardly on the ciphered content, producing an encryption outcome which coordinates the consequence of concurring operations performed on the plaintext, when decryption. An assessment calculation is added to encryption and decoding which works on cipher text. [1]

Dsouza et al., (2014) recommended the approach in which system receives property based security structure wherein all clients are confirmed and recognized by an arrangement of traits. At least one of these credits will be utilized to approve the personality of the client and to confirm the demand of the client by his traits and entitles the character related standards and arrangements [3]

Kai et al., (2013) talked about the respectability of client' information in the cloud which might be at risk because of the associated reasons. To begin with, the organizations which provide cloud services may mask information misfortune for keeping up a dishonor. Also the organizations may recover capacity by disposing of information that has not been or once in a while to the sparing storage room. [4]

Lee, J. H. (2016) proposed Dispersed versatility administration is one push to adapt to the expanding portable information activity. Another plan intended for secure confirmation with element burrowing is presented. Liu et al., (2015) discussed despite the fact that the plan just requires just a single authenticator for each square, it has two serious downsides. To begin with, since the confirmation procedure requires mystery material, there will be security issues while stretching. [5]

Bellessa et al., (2011) examined an inference-based device for network configuration named as NetODESSA. It is one of the extended method of allotted host-stage policy-compliance tracking system named as ODESSA. It is designed to allow the construction of bendy and resilient dynamic networks via network directors to frame general strategies by combining several runtime data with network activities. [2]

Chang Liu, Rajiv Ranjan, Chi Yang, et al, 2015 discussed despite the fact that the plan just requires a single authenticator for each square, it has two serious downsides. Since the confirmation procedure requires mystery material, there will be security issues while stretching. [6]

Praveena, A., & Sasikala, C. (2015) proposed a novel privacy-preserving mechanism that maintenances public auditing on shared data stored in the cloud. It verifies and control the data integrity. This research focused mainly on retrieving the security issues like privacy risk, scalability, access and efficient user revocation. With this motivation, the novel protection scheme is considered for different key management schemes. [7]

Mahesh, A., and Manimegalai, P. (2016) suggested fault tolerant and data immutability architecture to store and processing of data generated by social media/IoT and this method additionally uses large scale machine learning techniques such as pattern recognition for the intelligent reports. This architecture is also suitable for parallel processing of sensor data for quick decision making. As this architecture uses open source software context which that makes easy determine and communicate with other devices. [16]

Suganthi et al., (2015) discussed a method in which the user will get a mail affirmation which could be an arbitrary key created independently for each record and this is required to get and to utilize the document from the cloud. If the client is not legitimate he/she can't get the record since the haphazardly produced key is basic for the document. [8]

Xia et al., (2016) followed tree-based index structure. They also proposed a "Greedy Depth-first Search" algorithm for providing effective multi-keyword ranked search. For encryption purpose, secure kNN algorithm is utilized and the information is encoded before outsourcing for security prerequisites. Apart from accuracy and multi keyword search, the system concentrates more dynamic update on document collections. [10]

Jingbo et al, 2016 conversed a secure multi-keyword ranked search scheme over encrypted cloud data, which supports dynamic update operations like insert and delete. Explicitly, vector space model and TFxIDF model are combined in the index construction and query generation. The authors recommended "Greedy Depth-first Search" algorithm which uses special tree-based index structure. Owing this, the recommended scheme achieves sub-linear search time and deal with the insert and delete operations in the documents submissively. [14]

R. Gopinathan, P Manimegalai et al, 2016, proposed an energy and latency aware packet forwarding protocol which selects the forwarding nodes diligently to ensure reliability and uses the anycast forwarding technique to handle energy and latency in the network along with successful data delivery at the destination. [9]

Farahnakian et al., (2014) framed an architecture that manages the Physical Machine (PM) to regulate its status. It also optimizes the Virtual Machines (VM). Recent developing interest of Cloud Foundation has impressively expanded the energy utilization of server, which has turned into a basic issue. Hence, it is necessary to manage the energy consumption as important role. [11]

Garg et al., (2015) examined a single bit diagonal Pre-coding block with closed loop. The Multiple-Input Single-Output (MISO) is considered here for processing the pre-encoding units. The signal to noise ratio and pair wise error probability are considered here for error detection. Here, golden and silver code are considered as a block codes. Garg et al., (2016) further extended the research for orthogonal space-time block code with the Symbol Error Rate (SER) parameter. [12] [13]

3. Content arrangement characteristic based encryption (CA-CBE)

Normally, cloud environment consists of both hardware and software to perform a computing service. This process is defined as utilizing the computer resource to end up a task. Hence the cloud computing is a computing model, it is totally differed from the technology. In computing process security is an important aspect of conveying messages through cloud. From the literature survey it is identified that the efficient model is to be designed. Hence, the proposed plan is based on new CP-ABE alteration by further incorporating into the intermediate decryption convention for the client repudiation. To deal with the greatest client repudiation, the information placing away focus must get the client get to (or repudiation) list for each attribute gather, since generally denial can't produce results all things considered.

The mathematical equation for CA-CBE is given below.

- The Term 'F' denotes the data file to be outsourced, it is denoted as an arrangement of various blocks m1,...,mn ∈ Zp for complex prime (p).
- Next parameter is Message Authentication Code (MAC) which is represented as MAC(•)(•). It is represented as K×{0,1}∗ →{0,1}l where K denotes the key space.
- H (•), h (•) – cryptographic hash functions.

The proposed scheme has extended from the cryptographic background, it is represented as follows:

The bilinear mapping is represented by assuming the characteristic interrupted groups of prime (p) order, namely G1, G2 and GT. Similar to the has functions, g1 and g2 be the generators of G1 and G2, respectively.

As per Hubbard, D., & Sutton, M. (2010), the following properties are considered for bilinear map, which is represented as $e: G1 \times G2 \rightarrow GT$.

The proposed model CA-CBE for all schemes named as, $v \in G2$ and $a, b \in Zp$, $e(ua, v) = e(u, v)$.

This bilinearity implies that for any $u1, u2 \in G1, v \in G2$, $e(u1 \bullet u2, v) = e(u1, v) \bullet e(u2, v)$. Of curriculum, there exists an efficiently computable algorithm for computing e and the Characteristic should be non-trivial, i.e., e is nondegenerate: e (g1, g2) =6 1

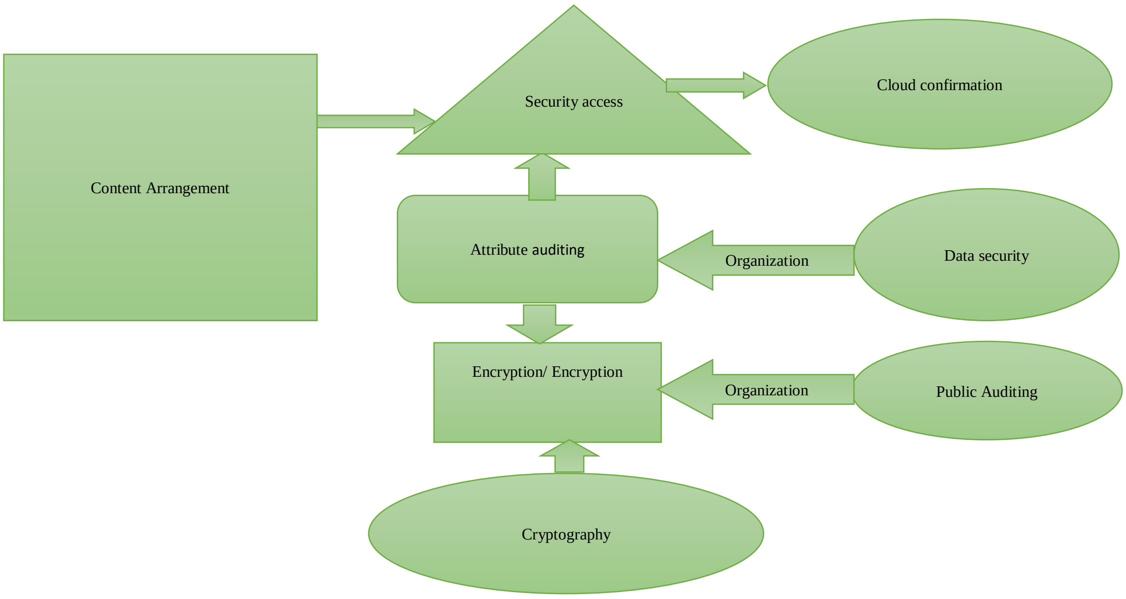

Figure 3.1: CA-CBE for public auditing

This information setting away focus knows the repudiation list which does not disregard the security prerequisites, since it is just permitted to re-encode the collected messages and can in no way, shape or acquire any data about the property keys of users. Attribute auditing perceives the security access with cloud confirmation.

3.1. Key assumption based on outsider auditing

When the request for data auditing is received from data owner or user to outsider auditing, it immediately request for the blocks of encrypted data from the cloud server. After receiving the data, it generates the key value for each block of encrypted files using the same CA-CBE algorithm used by a data owner to generate key. In the process of verification, it compares original encrypted key with outsider auditing key. If both match with each other, it indicates that the stored data on the cloud is complete i.e integrity is maintained and it is not tampered by any intruders. If it does not match, it indicates that the data integrity has been affected. The data owner is notified regarding the data integrity check results generated in the auditing process based on the matching of both keys.

Algorithm

```
Input: user data UD, Outsider auditing OA
Output: Integrity check result ICR
Begin
Get UD for Req.
Request from Encrypted data from Cloud server
Refresh the Cloud storage CS.
$CS = \sum \llbracket (CSi \in \backslash time) \cup Req.Resource \rrbracket$
Generate the key value
If user key = OA key
Data in cloud is complete and it is not tampered by any intruders
Else
Integrity of data in cloud is affected and data owner is notified.
End
```

General security and execution investigation demonstrates that the proposed model is greatly proficient and flexible compared to other calculating discontent, harmful information adjustment attack, and considerably server scheming assaults.

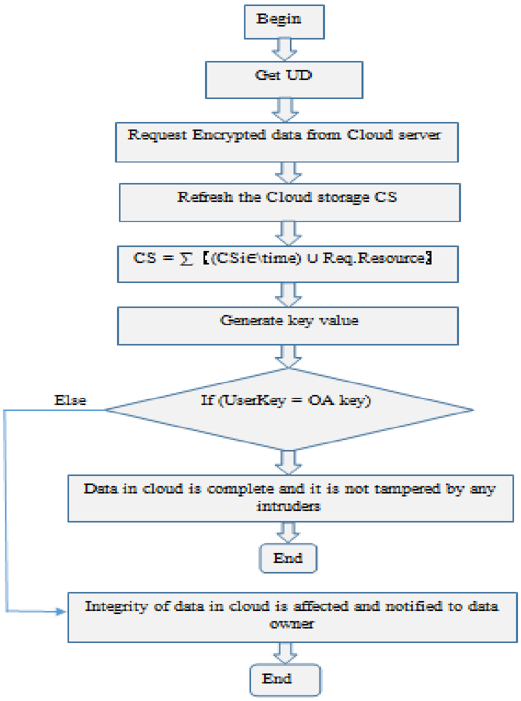
Begin
Get UD
Request Encrypted data from Cloud server
Refresh the Cloud storage CS
CS = ∑ 【(CSi∈\time) ∪ Req.Resource】
Generate key value
Else
If (UserKey = OA key)
Data in cloud is complete and it is not tampered by any intruders
End
Integrity of data in cloud is affected and notified to data owner
End

Figure 3.2: Flow diagram of outsider auditing

The above flow diagram is clearly depicts how the user data and key value are being used to analyse with outsider auditing. If the userkey matches the outsider auditing key, then all the data can be easily accessed by corresponding user in cloud. The data are split into parts and the encrypted format of the data is stored in cloud, thus maintaining the confidentiality of data. The data integrity is verified by outsider auditing on request of the data owner in cloud. General security and execution investigation demonstrates that the proposed plan is greatly capable and flexible against calculating discontent, harmful info adjustment attack, and considerably server scheming assaults.

3.2. Content arrangement characteristic based encryption using cryptography

Cryptography key appropriation is a measure of consideration from the specialists, as a strategy authorizing substantial. It is dynamic gatherings of clients to set up gathering keys over the untrustworthy system for secure multicast correspondence. In such plans, time is separated into ages called as sessions. Towards the start of every session, a Gathering key transmits message as a communication, keeping in mind the end goal to give a typical key to every individual from the gathering. Each client, having a place with the gathering, registers the gathering key utilizing the message and some private data.

Algorithm

```
Input: Cloud Table CT
Output: Key Table KT
Step 1: Start
Step 2: Create encryption data ED
Step 3: Broadcast key for cloud BKC
Step 4: Start encryption process EP
Step 5: While Timer is running
Receive all encryption data.
Extract data details and location key.
Updateable for each entry
$Kt(i) = BKC\{EP - ED * CT)$
End
Step 6: Stop
```

If some of the communicated message get lost, then clients are still apt for improving the gathering key for that session by utilizing the message they got at the start of a past session and the message they get the start of a resulting one, without asking for extra transmission from the group manager.

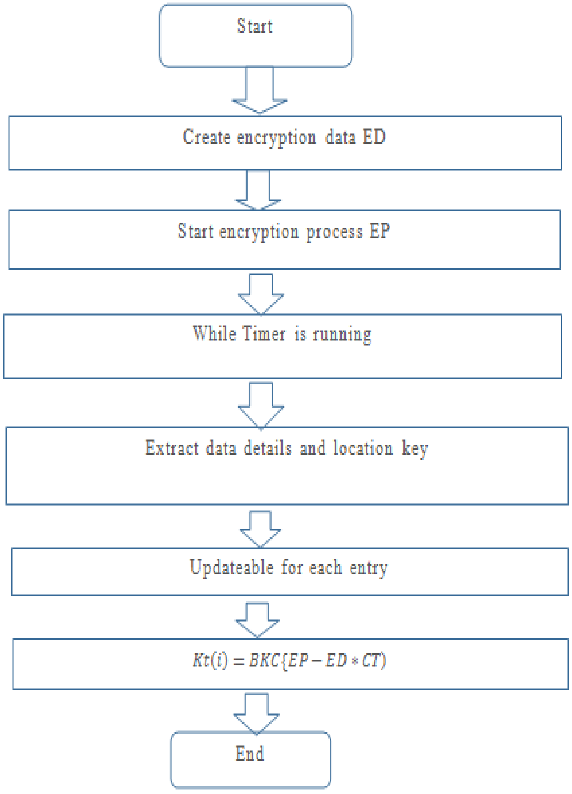
Start
Create encryption data ED
Start encryption process EP
While Timer is running
Extract data details and location key
Updateable for each entry
$Kt(i) = BKC\{EP - ED * CT)$
End

Figure 3.3: Flow chart of CA-CBE

Key Delivering for CA-CBE, auditing and the data-storing midpoint are complicated in the user key distributing protocol. The client is required to contact the two gatherings before getting an arrangement of keys. The reviewer is responsible for of verifying a client and issuing credit keys to the user, whether the client is qualified for the characteristics. The cloud key is produced through the protected convention between the reviewer and the information pushing guy away effort. They take part in the number of manipulating secure convention with top anonymous keys of their own, and issue free key segments to a client. At that point, the client can create the entire anonymous keys with the key segments independently got from the two specialists. The safe convention stops them from knowing each other's lord privileged insights so that none of them can produce the entire anonymous keys of a client alone.

4. Result and discussion

The proposed Content Arrangement Characteristic Based Encryption has been designed, implemented and tested using different simulation scenarios. The method has been evaluated for its performance using the simulator and the performance of the proposed mechanism has been evaluated.

The proposed system provided improved information security and secrecy in the information sharing framework against any framework administrators without relating certifications. The proposed plan can make a quick client denial on each characteristic set while taking the full favorable position of the adaptable which is to get control given by the cipher content arrangement trait based encryption.

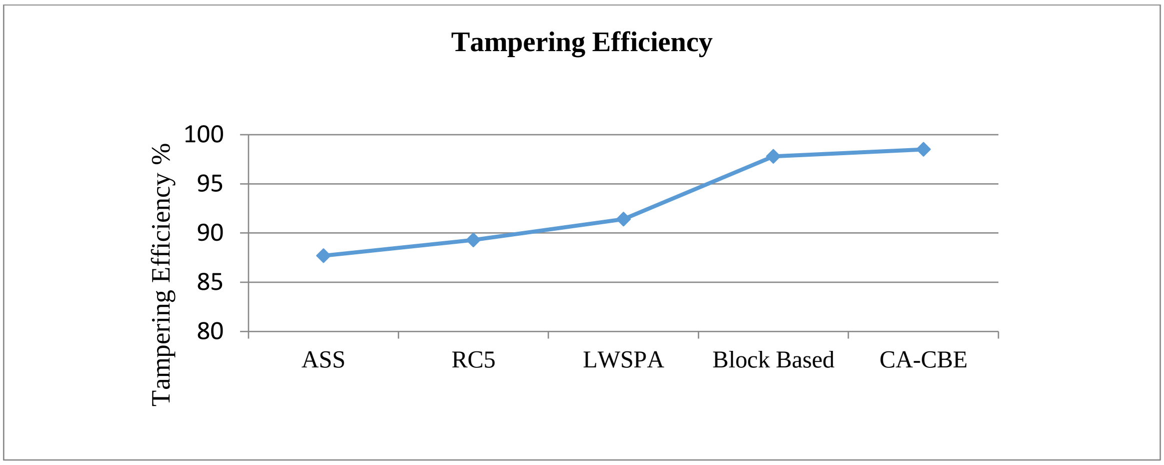

Figure 4.1: Correlation of tampering efficiency

The Figure 4.1 demonstrates the tampering productivity delivered by various techniques and it demonstrates that the proposed CA-CBE has created effective outcomes than different strategies.

Table 4.1: Comparison Table of Different Techniques

Techniques	**Auditing accuracy**
ASS	87.7
RC5	89.3
LWSPA	91.4
Block Based	97.8
CA-CBE	98.5

Parameter tampering could be a variety of Web-based assault in which parameters within the Uniform Resource locator (URL) or online page form field data entered by a consumer are modified while not that client's approval. This indicates the program, connection, page or site other than the one the client plans (despite the fact that it might appear to be identical to the easygoing onlooker). Auditability for storage security (ASS), RC5, Light Weight Single Parametric Approach (LWSPA), Block based and CA-CBE methods are compared and the values are given above.

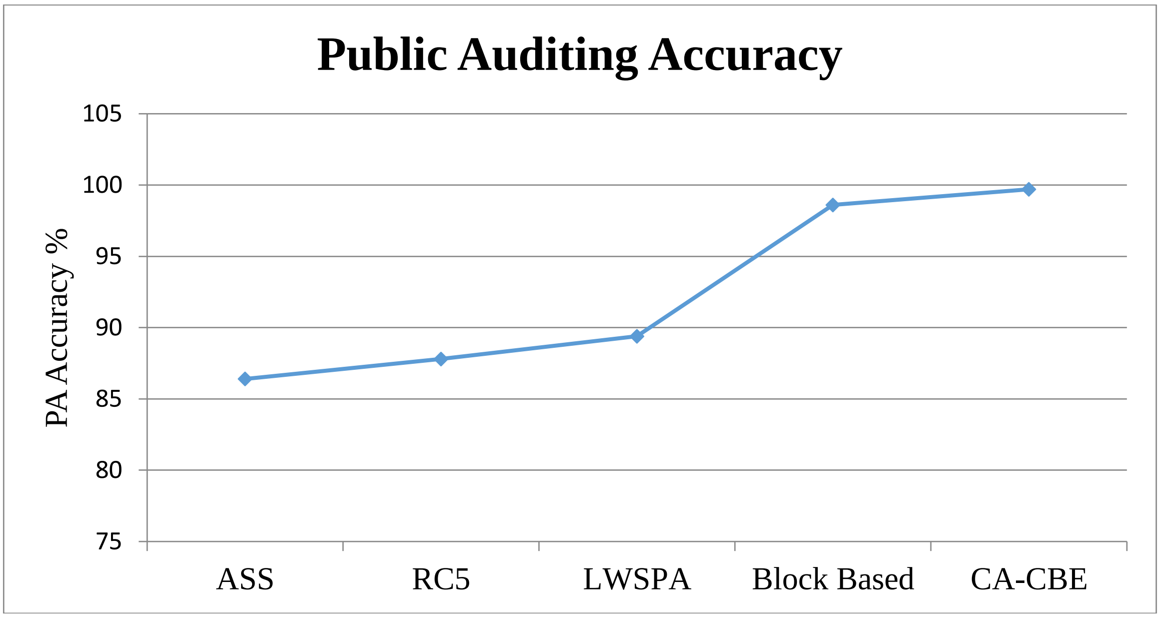

Figure 4.2: Correlation of Auditing Accuracy

The Figure 4.2 demonstrates the outcome on public auditing accuracy created by various techniques and it indicates obviously that the proposed strategy has delivered highest accuracy than other different strategies.

Table 4.2: Comparison Table for Different Techniques

Techniques	**Auditing accuracy**
ASS	86.4
RC5	87.8
LWSPA	89.5
Block Based	94.3
CA-CBE	98.6

The time complexity is one of the measure normally estimated for calculating the number of fundamental operations to test the algorithm. It is determined by an elementary operation that depends on fixed amount of time to perform the whole operation. Hence, it is important to analyze this factor because the proposing algorithm may get varied with several constant factors. It may depends upon the algorithmic performance with different input size. For example, the commonly representation of worst-case time complexity is denoted as T(n), where, ‘n’ is termed as the maximum time taken on varies input of size n. Similarly, the less common is stated as explicitly, it is the measure of average-case complexity. For instance, an algorithm with T (n) = O (n) is called a time complexity.

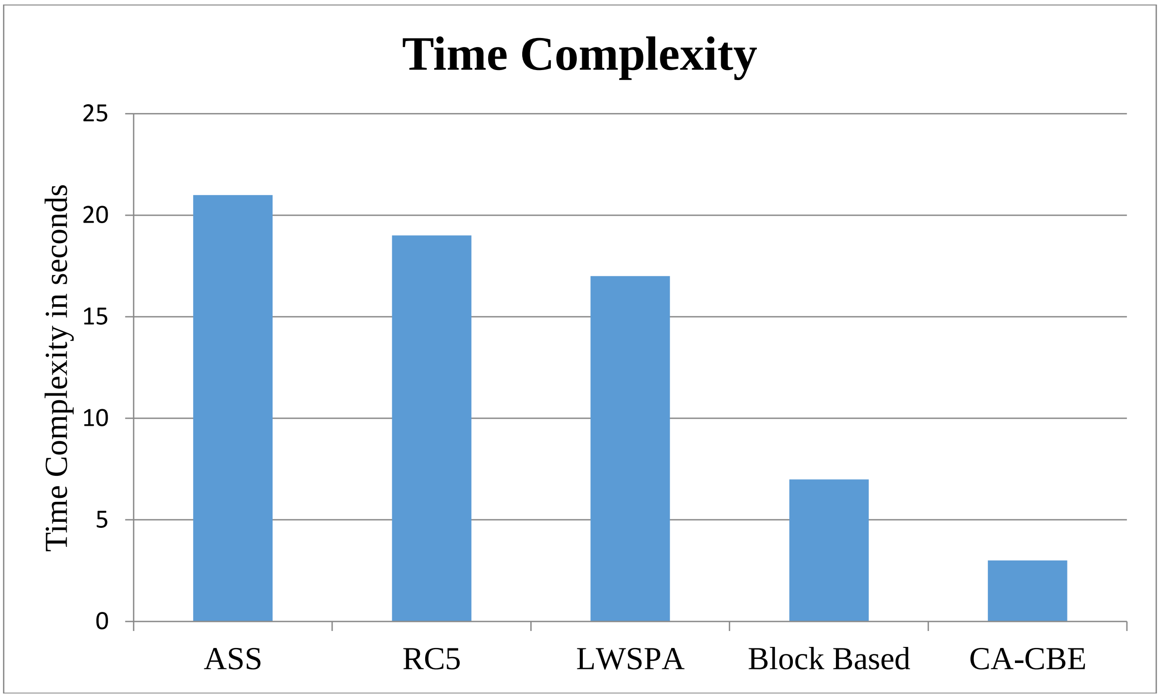

Figure 4.3: Correlation of time complexity

Figure 4.3 demonstrates the similar outcome on time complexity in confirmation and the outcome demonstrates that the proposed strategy has diminished the time complexity as compared to different strategies mentioned above.

5. Conclusion

The implementation of getting arrangements and support of strategy updates are critical testing issues in the information sharing frameworks. In an attribute based information sharing plan, the implementation of time information and getting the control, is carried out by auditing the information in the sharing framework. The proposed system collaborates and highlights a key issuing instrument that evaluates key details among the key time. The client secret keys are created through a safe two-party calculation with the end goal that any inquisitive key time focus or information away focus can't infer the private keys exclusively. In this manner, the proposed plot accomplishes more secure and CA-CBE information get control in the information sharing framework. The exhibited and the proposed plan is productive and adaptable to maintain integrity of the client information in the information sharing framework.

References

[1] Tajan L, Westhoff D, Reuter CA & Armknecht F, “Private information retrieval and Searchable Encryption for privacy-preserving multi-client cloud auditing”, *11th International Conference for Internet Technology and Secured Transactions (ICITST),* pp. 162-169, (2016).

[2] Bellessa J, Kroske E, Farivar R, Montanari M, Larson K & Campbell RH, “NetODESSA: Dynamic policy enforcement in cloud networks”, *30th IEEE Symposium on Reliable Distributed Systems Workshops (SRDSW),* pp. 57-61, (2011).

[3] Dsouza C, Ahn GJ & Taguinod M, “Policy-driven security management for fog computing: Preliminary framework and a case study”, *IEEE 15th International Conference on Information Reuse and Integration (IRI),* pp. 16-23, (2014)

[4] Kai H, Chuanhe H, Jinhai W, Hao Z, Xi C, Yilong L, Lianzhen Z & Bin W, “An efficient public batch auditing protocol for data security in multi-cloud storage”, *8th ChinaGrid Annual Conference (ChinaGrid),* pp. 51-56, (2013).

[5] Lee JH, “Secure authentication with dynamic tunneling in distributed IP mobility management”, *IEEE Wireless Communications*, Vol.23, No.5, pp.38-43, (2016).

[6] Liu C, Ranjan R, Yang C, Zhang X, Wang L & Chen J, “MuR-DPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud”, *IEEE Transactions on Computers*, Vol.64, No.9, pp.2609-2622, (2015).

[7] Praveena A & Sasikala C, “Multi authority attribute based encryption against data integrity and scalability issues in cloud data services”, *International Conference on Innovations in Information, Embedded and Communication Systems,* pp. 1-5, (2015).

[8] Suganthi J, Ananthi J & Archana S, “Privacy preservation and public auditing for cloud data using ASS in multi-cloud”, *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS),* pp.1-6, (2015).

[9] Gopinathan R & Manimegalai P, “Energy and Latency Aware Position Based Packet Forwarding Protocol for Wireless Sensor Networks”, *Republication*, (2016).

[10] Xia Z, Wang X, Sun X & Wang Q, “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data”, *IEEE Transactions on Parallel and Distributed Systems*, Vol.27, No.2, pp.340-352, (2016).

[11] Farahnakian F, Pahikkala T, Liljeberg P & Plosila J, “Hierarchical agent-based architecture for resource management in cloud data centers”, *IEEE 7th International Conference on Cloud Computing (CLOUD),* pp. 928-929, (2014).

[12] Garg A, Venu V & Bhatnagar MR, “One bit feedback based diagonal precoding for non-orthogonal space-time block codes”, *IEEE Wireless Communications Letters*, Vol.4, No.5, pp.573-576, (2015).

[13] Surendar, A., George, A.”A real-time searching and sequencing assembly platform based on an FPGA implementation for Bioinformatics applications”,(2016) International Journal of Pharma and Bio Sciences, 7 (4), pp. B642-B647.

[14] Surendar, A., Arun, M.”FPGA based multi-level architecture for next generation DNA sequencing”,(2016) Biomedical Research (India), 2016, pp. S75-S79.

[15] Surendar, A., Arun, M., Basha, A.M.”Micro sequence identification of bioinformatics data using pattern mining techniques in FPGA hardware implementation”,(2016) Asian Journal of Information Technology, 15 (1), pp. 76-81.

[16] Prabu, G., Surendar, A.”Virus detection by using a pattern matching algorithm for network security”,(2015) International Journal of Applied Engineering Research, 10 (10), pp. 9565-9569.

[17] Mahesh A & Manimegalai P, “An efficient data processing architecture for smart environments using large scale machine learning”, IIOAB Journal, Special Issue, Emerging Technologies in Networking and Security, Vol.7, No.9, pp.795-803, (2016).

[18] Kaseb AS, Mohan A & Lu YH, “Cloud resource management for image and video analysis of big data from network cameras”, *International Conference on Cloud Computing and Big Data (CCBD),* pp. 287-294, (2015).

[19] Li J, "Optimal resource capacity management for stochastic loss network systems with applications in clouds and data centers", *IEEE 55th Conference on Decision and Control*, pp.5384-5389, (2016).

[20] Salas-Duarte S, Araujo-Vargas I, Flores-Alcotzi O, Ramirez-Hernandez J & Del Muro-Cuellar B, "Experimental verification of a one-step ahead current control scheme for an active rectifier", *IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)*, pp. 1-6, (2014).

[21] Singla P, Kumar P, Das A, Sardana V & Sardana HK, "Image registration: A pre-step in patient's position verification in radiation therapy", *International Conference on Image Information Processing (ICIIP)*, pp. 1-4.

[22] Wadhwa S, Ahmad M & Vijay H, "Chaotic hash function based plain-image dependent block ciphering technique", *International Conference on Advances in Computing, Communications and Informatics*, pp. 633-637, (2016).

[23] Xiao W, Shi, G, Li, B, Xu J & Wu F, "Fast Hash-based Inter Block Matching for Screen Content Coding", *IEEE Transactions on Circuits and Systems for Video Technology*, (2016).