International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 11294-11301

Ensemble Secure Communication Protocol (ESCP) for Data Storage and Retrieval in Private Cloud

A.Anusha Priya[1] and R.Gunasundari[2]

[1]Research Scholar, [2]Associate Professor
[1,2,] Department of Information Technology, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India.
[1]Orcid Id:0000-0001-6050-169X, [2]Orcid Id: 0000-0003-4157-285X

Abstract

Cloud computing is the recent and thrust research area in the field of information technology. Cloud computing offers a paradigm shift in four major areas such as compute, storage, networking and applications. This research work aims to design and develop the Ensemble Secure Communication Protocol (ESCP) for efficient data storage and retrieval among the private cloud. ESCP has 3 stages. The first conscription stage is used to setup / deploy the private cloud computing environment. The second stage is an authentication and a key sharing stage validates the user with the help of encryption and decryption mechanisms. Finally, at the secure communication stage, the data are stored and retrieved. Matlab tool is used for implementation. Performance metrics such as time taken for encryption, time taken for decryption, overall elapsed time and time taken for data retrieval are taken into account. Performance analysis is also conducted and from the obtained results it is evident that the proposed ESCP outperforms than the existing mechanisms.

Keywords: innovation policy, innovative capacity, innovation strategy, competitive advantage, road transport enterprise, benchmarking.

INTRODUCTION

Cloud computing is a promising data innovation basic outline for both endeavors and people that impels a beautiful data storage and intuitive thought with evident preferences, including on-request self-administrations, omnipresent system get to, and area autonomous asset pooling. Thus, security and protection issues are alluring key worries with the developing notoriety of cloud administrations. Conventionalist common security approaches used for the most part concentrate on the solid confirmation to comprehend that a client can remotely get to its own particular data in on-request mode. Next with the assortment of the application necessities, clients most likely will crave and share each other's approved data fields to accomplish productive compensation, which brings new security and protection challenges for the private cloud storage. Secured circulated data storage in the throng remote data storage by the utilization of Storage-as-a-Service (STaaS) benefit model is increasing significantly the research enthusiasm for as far back as decade. A few cloud sellers have given striking storage benefit help to invest with tremendous and adaptable cloud-based storage spaces for clients, for example, Amazon, Drop box, Google Drive, and Microsoft's One Drive [7, 11, 14] .Again, the security issue sourced by the operations on cloud side is yet an obstacle of making utilization of STaaS for private cloud condition [1, 5, 6, 8, 23].A inspiration illustration that points of interest the key piece of the proposed model is securing data bundles with the delicate data. The procedure has part data parcels and data bundles recoveries. This situation happens in the money related industry, social insurance and so on in which clients' delicate data should be exceedingly ensured on the cloud condition. It is assumed that there are two remote cloud storage servers, A and B. There is an info data D that is 0100 1010 0101 1110. The proposed display means to store data D in appropriated form on to the cloud server A and B and guarantee cloud administrators at An and B should not straightforwardly get to the data. The storage procedure additionally requires guaranteeing both the high security and low inertness and overhead prerequisites.

LITERATURE REVIEW

Security issues have entered into the most layers of cloud computing, from systems to framework administrations [21]. Numerous security issues in systems and information stockpiling are additionally pertinent to cloud computing because of the interconnections between the specialized applications, for example, utilizing Virtual Machine (VM). Earlier inquires the investigated about the security issues and arrangements in numerous points of view. Initially, the information administration security is a part of securing information in cloud computing, which frequently concentrate on encryption arrangements or information groupings with the end goal of the security [16,18] . Some methodologies have been created to guarantee the protected question prepared for Resource Description Framework (RDF, for example, utilizing extensible Access Control Markup Language (XACML) administration approach [4]. Also, a specific information encryption is viewed as a method for decreasing computing cost while ensuring information in clouds. For instance, ordering information in the assorted positions

utilizing accessible encryption is an approach for clients to change whether the information should be encoded [3,12]. In any case, the most current information administration techniques accept that the cloud administrators do not manhandle the information or have restricted access to the information. There is a probability of recovering data despite the fact that the information are scrambled on the cloud side, in a few circumstances. Next, observing and ensuring information stockpiling is another measurement in securing cloud information, which considers the information handling or operations happened in the clouds. It infers that the cloud administrators' practices are analyzed or investigated. One of the methodologies is utilizing Attributed-Based Encryption (ABE) to secure the protection data when the information are shared among the different clouds [15,20] . Notwithstanding, confining cloud administrators' access scale can likewise bring about different issues, for example, information incorporation and information soundness [10,17]. Dangers of information harm or operation disappointment rate will be expanded if the cloud specialist co-ops are completely blocked [5, 13, 22]. Along these lines, from the viewpoint of information stockpiling, the inconsistencies between the security insurance and information handling are hard to be unraveled. It is sought to secure information on cloud servers by utilizing encryption-arranged methodologies. Past inquires have additionally tended to this field, for example, Fully Homomorphic Encryption (FHE) [19] and ABE. Notwithstanding this sort of secure components can viably shield information from the objective aggressors, for example, outer noxious activities and inner shameful operations; in any case, the effectiveness of the information preparing can be a negative affect because of the extra calculations [2,9]. The following segment addresses certain exploration scope managed in the literary works.

PROPOSED WORK

In this research work a protocol that offers authentication mechanism, key exchange scheme, and secure communication. The proposed protocol hence named as an Ensemble Secure Communication Protocol (ESCP) for private cloud. In the private cloud, architecture several “data terminals” are present that will both act as sources and recipients of data. A static “data center terminal” is used to harmonize the communication of each terminal in its read range and pass the data to a “router”. The router consequently passes the information to the cloud through the “Network Gateway” to be utilized. The data terminals are constrained in computational resources, while the data center terminals and all the other higher-level terminals are relatively resourceful. It is assumed that the data center terminals and the data terminals are distributed that each data terminal is within the read range so that one data center terminal at all times. Each data terminal, data center terminal, and router possess a Actually Inclinable Function (AIF) instance that is used to authenticate them to the data center terminal, router, and network gateway, respectively.

The proposed ESCP involves the below mentioned stages. At first, a **Conscription Stage** is done, for each data terminal which is being managed by a given data center terminal. This procedure creates a challenge-response pair (CRP) database for the AIF contained in each terminal in the data center terminal whether corresponding to the data terminal. When two terminals intend to communicate, their common data center terminal first authenticates them. After that motivates to create their public/private key pairs, and then enables secure key sharing. This is called as the **Authentication and Key Sharing Stage.** To end with, in the **Secure Communication Stage**, the two terminals send and receive the information securely over the network using the keys, without any intervention of the data center. At a point where a data terminal shifts to a new location so that it has to be managed by a new data center terminal, the authentication procedure need to be done between the data terminal and new data center terminal administering it.

It has been assumed that each data terminal holds the address of the data center terminal known as the “home address” in which it is enrolled. When it moves to the domain of a new data center terminal, a “handoff mechanism” reassigns the terminal to the new data center. To start it, the data terminal sends the authentication request to the new data center terminal along with its home address. If the address is within the range of the router to which the new data center belongs, then it randomly chooses two challenges and sends an encrypted message to the old data center asking for the responses corresponding to the data terminal’s CRP database. As these two data centers are under the same router, it can be assumed that they already have session key pairs or can create a pair by authenticating to the router. Once the old data center receives the message, it retrieves the responses from the data terminal’s CRP database and forwards it back to the new data center. Consequently, the new data center authenticates the data terminal using these two challenge-response pairs.

However, if the old data center resides in the domain of a different router, then the new data center forwards the request to its router. It finds out the router of the old data center and sends the message to it (using their public/private key pairs). The router of the old data center retrieves the responses from it and again forwards them to the router of the new data center. It comes back to the new data center later and is used for authenticating the data terminal by the new data center. Once authentication is done, the data terminal can establish key pairs with any other data terminal in the new data center’s domain.

The proposed scheme needs that the communicating parties need to concur on several mathematical parameters before initiating communication. For some large prime value p , two

groups G_1, G_2 of order p are created, and a tolerable bilinear map $\hat{e}: G_1 \times G_1 \to G_2$ is defined over these two groups. We also need to choose four secure cryptographic hash functions:

$(1) H_1: \{0,1\}^n \to G_1^*; (2) H_2: G_2 \to \{0,1\}^n; (3) H_3: \{0,1\}^n \times \{0,1\}^n \to Z_p^*$, where Z_p^* is a set of nonnegative integers less than p and coprime to p; and $(4) H_4: \{0,1\}^n \to \{0,1\}^n$, where n is the bit length of the message. So the public mathematical parameters are $< p, G_1, G_2, \hat{e}, n, H_1, H_2, H_3, H_4 >$.

Conscription Stage

Sooner than positioning the terminals in the cloud infrastructure, the conscription stage is executed for each terminal in a secure and trusted environment. In the conscription stage certain preliminaries are carried out.

- The data center sends a random challenge C to the terminal.

- The terminal applies the challenge C to its AIF and generates the output $R = AIF(C)$ and returns it to the data center.

- The data center stores the response along with the challenge by appending $< C, R >$ to its database.

- This procedure is repeated K times which is predefined according to the memory capacity of the data center.

Towards the end of the conscription stage for a given terminal, the data center terminal supervising the data terminal has a CRP database with k CRPs for the terminal. Here it is assumed that the data center stores the CRP in a secure database that cannot be accessed by the attacker, and that the data center is sufficiently resourceful to implement secure databases.

Authentication and Key Sharing Stage

The second stage of this protocol performing the authentication and key sharing are described as follows and shown in Figure 3:

—At first, $Ter\min al_1$ initiates a request to inform the data center about its willingness to send a message to $Ter\min al_2$ and to supervise the communication.

—The data center chooses two challenges C_1 and C_2 randomly from the stored AIF CRP database of $Ter\min al_1$, C_3 and C_4 randomly from the stored AIF CRP database of $Node_2$. The data center terminal also fixes a timestamp (*TS*) for initializing the protocol and performs the following computations:

$$\Delta_1 = H_1(R_1 \| R_2 \| TS)$$

$$\Delta_2 = H_1(R_3 \| R_4 \| TS)$$

$$TS'_1 = TS \oplus (R_1 \| R_2)$$

$$TS'_2 = TS \oplus (R_3 \| R_4) \qquad (4)$$

Where $R_1, R_2, R_3,$ and R_4 are the AIF responses corresponding to the challenges $C_1, C_2, C_3,$ and C_4. Note that Δ_1 and Δ_2 are calculated as elements of G_1^*.

—The data center terminal then sends (C_1, C_2, TS'_1) to $Ter\min al_1$ and $(Ter\min al_1, C_3, C_4, TS'_2)$ to $Ter\min al_2$.

—After receiving the message from the data center, $Ter\min al_1$ calculates

$$TS = TS'_1 \oplus (AIF_1(C_1) \| AIF_1(C_2))$$

$$ID_1 = H_1(AIF_1(C_1) \| AIF_1(C_2) \| TS)$$

$$P_1 = H_1(C_1 \oplus C_2)$$

Thus $Ter\min al_1$ applies the challenges C_1, C_2 to its AIF instance, gets the corresponding responses, and calculates the value of $ID_1 \in G_1^*$, which ideally must be equal to Δ_1.

—Next, $Ter\min al_1$ randomly chooses a value t such that $t \in R Z_q^*$ and computes

$$K1_{PUB} = t.P_1$$

$$K1_{PRV} = t.ID_1$$

$$d_1 = H_4(AIF_1(C_1) \oplus AIF_1(C_2) \oplus ID_1 \oplus P_1 \oplus K1_{PUB} \oplus TS)$$

.

—$Ter\min al_1$ then sends a message to the data center, which contains $ID_1, P_1, K1_{PUB}, d_1$. Note

that $K1_{PUB}$ and $K1_{PRV}$ act as the public and private key for *Terminal*1, respectively.

—$Ter\min al_2$ Also performs operations similar to $Node_1$:

$$TS = TS'_2 \oplus \left(AIF_2(C_3) \| AIF_2(C_4)\right)$$

$$ID_2 = H_1\left(AIF_2(C_3) \| AIF_2(C_4) \| TS\right)$$

$$P_2 = H_1(C_3 \oplus C_4)$$

Thus, $Ter\min al_2$ applies the challenges C_3, C_4 to its AIF instance, gets the corresponding responses, and calculates the value of $ID_2 \in G_1^*$, which ideally must be equal to Δ_2.

—Next, it randomly chooses a value s such that $s \in RZ_q^*$ and computes

$$K2_{PRV} = s.ID_2$$
$$K2_{PUB} = s.P_2$$

$$d_2 = H_4\left(AIF_2(C_3) \oplus AIF_2(C_4) \oplus ID_2 \oplus P_2 \oplus K2_{PUB} \oplus TS\right).$$

As in the case of $Ter\min al_1$, $K2_{PUB}$ and $K2_{PRV}$ act as the public and private key for $Node_2$, respectively.

—$Ter\min al_2$ sends a message to the data center, which contains $(ID_2, P_2, K2_{PUB}, d_2)$.

—After receiving messages from both $Ter\min al_1$ and $Ter\min al_2$, the data center terminal needs to authenticate them individually and also check whether the public key truly belongs to the correct terminal claiming it. To ensure this, it first checks if $ID_1 = \Delta_1$, and if the test passes, then data terminal ,*Terminal*1 is authenticated.

—Correspondingly, if the data center finds $ID_2 = \Delta_2$, then the data terminal $Ter\min al_2$ is authenticated. Additionally, if $H_4\left(R_3 \oplus R_4 \oplus ID_2 \oplus P_2 \oplus K2_{PUB} \oplus TS\right) = d_1$, then the public key is also authentic and it belongs to $Node_2$. Hence, the data center terminal accepts it.

—When the data center completes authentication for both parties, it transmits the public keys to their corresponding receivers. For that, it calculates

$$d_3 = H_4\left(R_1 \oplus R_2 \oplus ID_2 \oplus P_2 \oplus K2_{PUB}\right) d_4$$
$$= H_4\left(R_3 \oplus R_4 \oplus ID_1 \oplus P_1 \oplus K1_{PUB}\right)$$

—Finally, the data center terminal sends $Ter\min al_1$ and $Ter\min al_2$ two messages containing $(ID_2, P_2, K2_{PUB}, d_3)$ and $(ID_1, P_1, K1_{PUB}, d_4)$, respectively.

—Once the message from the data center terminal is received by $Ter\min al_1$, it calculates $H_4(PUF_1(C_1) \oplus PUF_1(C_2) \oplus ID_2 \oplus P_2 \oplus K2_{PUB})$. If it equals d_3, then $Ter\min al_1$ is assured that the message is truly generated by the data center terminal, and thus $Ter\min al_1$ accepts $Ter\min al_2$'s public key.

—similarly, $Node_2$ calculates $H_4(PUF_2(C_3) \oplus PUF_2(C_4) \oplus ID_1 \oplus P_1 \oplus K1_{PUB})$. If it equals d_4, then $Ter\min al_2$ is assured that the message is truly generated by the data center terminal, and $Ter\min al_1$'s public key is accepted by $Ter\min al_2$.

Secure Communication Stage

The secure communication stage consists of the following steps:

—First, $Ter\min al_1$ (the sender) executes the following steps:

—It selects the message M and a nonce. Both of the entities are n-bit long. It then calculate the following: $V = \left(H_2\left(\hat{e}\left(K1_{PRV}, p_1\right)\right)\right)$. Note that since $K1_{PRV} = t.ID_1$, it follows that $\hat{e}\left(K1_{PRV}, p_1\right) = \hat{e}\left(t.ID_1, P_1\right) = \hat{e}\left(ID_1, P_1\right)^t \in G_2$.

—$Ter\min al_1$ then calculates $W = H_3\left(nonce \| M\right)$ and $X = W.P_2$.

—$Ter\min al_1$ Further calculates $Y = nonce \oplus H_2\left(\hat{e}\left(K2_{PUB}, ID_2\right)^W\right)$
$= nonce \oplus H_2\left(\hat{e}\left(s.P_2, ID_2\right)^W\right) = nonce \oplus H_2\left(\hat{e}\left(P_2, ID_2\right)^{s.W}\right)$
, and

—$Z = M \oplus H_4(nonce) \oplus V$.

—Finally, for the plain text M, $Node_1$ creates the cipher text as the 3-tuple (X, Y, Z), and sends to $Ter\min al_2$.

—Once $Ter\min al_2$ receives the cipher text, it follows these steps:

—If $X \notin G_1^*, Ter\min al_2$, rejects the message; otherwise, it calculates the following three values:

—$nonce' = Y \oplus H_2\left(\hat{e}\left(X, K2_{PRV}\right)\right)$

$$= Y \oplus H_2\left(\hat{e}\left(W.P_2, s.ID_2\right)\right)$$
$$= Y \oplus H_2\left(\hat{e}\left(P_2, ID_2\right)^{s.W}\right)$$

— $M' = Z \oplus H_4(nonce') \oplus H_2\left(\hat{e}\left(ID_1, K1_{PUB}\right)\right)$

$$= Z \oplus H_4(nonce') \oplus H_2\left(\hat{e}\left(ID_1, t.P_1\right)\right)$$

$$= Z \oplus H_4(nonce') \oplus H_2\left(\hat{e}\left(ID_1, P_1\right)^t\right), \text{ and}$$

— $W' = H_3\left(nonce' \| M'\right)$.

—If X equals $W'.P_2$, $Ter\min al_2$ accepts M' as the message; otherwise, it rejects the message.

—Now, if $Node_1$ does not send the message, then the value of $H_2\left(\hat{e}\left(K1_{PUB}, ID_1\right)\right)$ cannot be equal to V. That, in turn, implies that $X \neq W'.P_2$. Therefore, $Ter\min al_2$ never accepts an incorrect message M' in place of M. And if it accepts the message, then $Ter\min al_1$ cannot deny that it does not send it.

Security Model

The following potential attacks which threaten the security of the cloud data are given in this section.

1. Unauthorized accessing: In this kind of threat for security, the adversaries intend at thieving the key to decrypt the cloud data without the data owner's access permission. The adversaries are probably the outside attackers.

2. Collusive attack: In this kind of threat the collusion between the untrusted cloud server and the malicious cloud user is deployed. It is presumed that the cloud server probably will collude with a user who has restricted access for helping him to keep hold of the data access license to menace the security of the private cloud data sharing system.

RESULTS AND DISCUSSIONS

The experimental machine is a HP with Intel Pentium CPU N3700, 8GB DDR3 memory and SATA2 500 GB hard disk. In this experiment, different file types with the sizes range from 10MB to 50 MB are used. Performance metrics such as time taken for encryption, time taken for decryption, overall elapsed time and time taken for data retrieval are chosen. The proposed D2S2M is compared with two existing mechanisms proposed by L.Wei et al (2014) and Q.Liu et al (2014). The simulation environment is portrayed in the Fig.1.

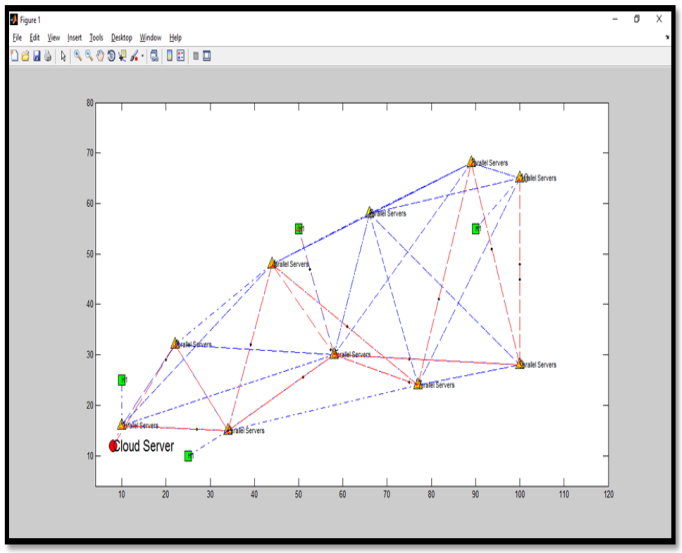

Figure 1: Simulation Environment

The results are shown below.

Table 1: Time Taken for Encryption

Data Size (in MB)	Time Taken for Encryption (in milliseconds)		
	ESCP (Proposed)	Q.Liu et al (2014)	L.Wei et al (2014)
10	21134	38172	45821
20	40948	54834	67299
30	57192	73389	86244
40	69834	94893	104332
50	93997	125732	138748

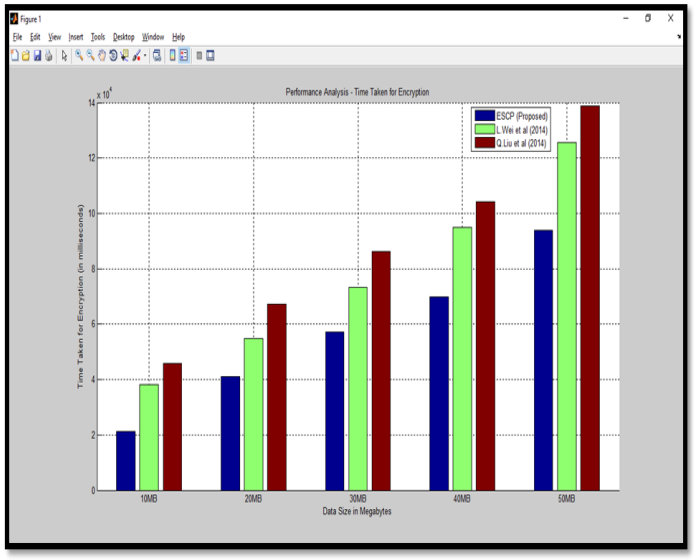

Figure 2: Performance Analysis in terms of Time Taken for Encryption

Table 2: Time Taken for Decryption

Data Size (in MB)	Time Taken for Decryption (in milliseconds)		
	ESCP (Proposed)	Q.Liu et al (2014)	L.Wei et al (2014)
10	20843	37384	46294
20	39745	53173	68013
30	56738	72094	86115
40	68116	93126	104274
50	93997	126743	137938

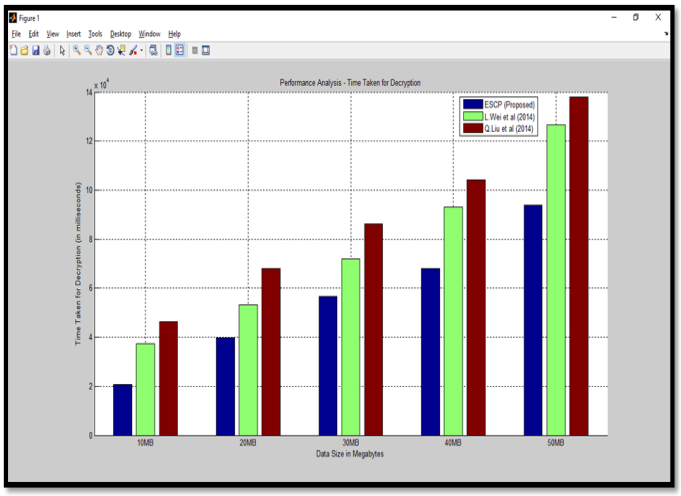

Figure 3: Performance Analysis in terms of Time Taken for Decryption

Table 3: Overall Elapsed Time

Data Size (in MB)	Overall Elapsed Time (in milliseconds)		
	ESCP (Proposed)	Q.Liu et al (2014)	L.Wei et al (2014)
10	44394	76550	93109
20	84183	109291	136596
30	96491	146850	173726
40	117564	189765	210352
50	157294	254421	278632

Table 4: Time Taken for Data Retrieval

Data Size (in MB)	Time Taken for Data Retrieval (in seconds)		
	ESCP (Proposed)	Q.Liu et al (2014)	L.Wei et al (2014)
10	2.2374	6.3845	9.6538
20	3.1836	7.1264	8.0265
30	3.3849	5.9475	8.9472
40	3.2991	6.8164	9.0472
50	3.4532	7.0372	8.5839

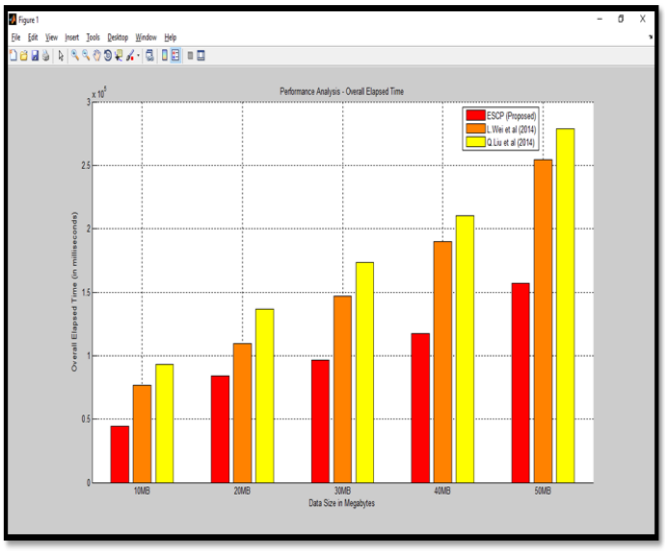

Figure 4: Performance Analysis in terms of Overall Elapsed Time

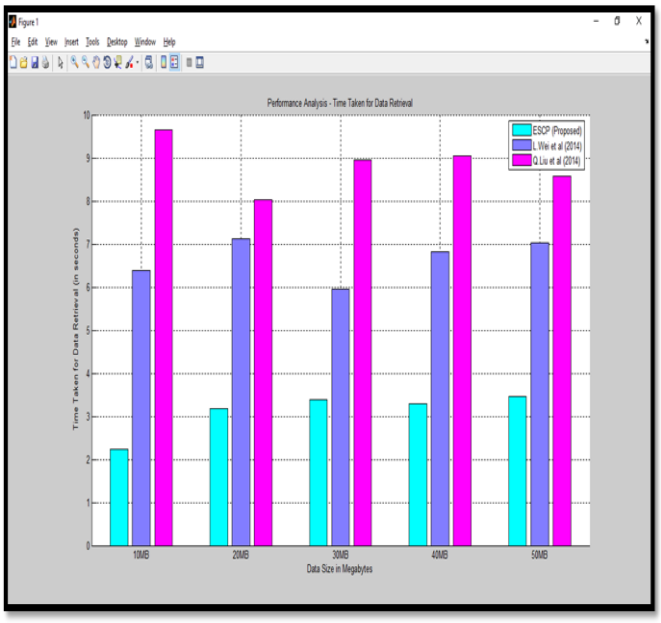

Figure 5: Performance Analysis in terms of Time Taken for Data Retrieval

CONCLUSION

The proposed ESCP consists of three important stages. Initially conscription stage takes care of the overall deployment of the private cloud. Next stage deals with authentication and key generation. Finally, secure communication takes place by which data are stored in the cloud servers (data centers) and retrieved by the terminal nodes. MATLAB simulations are carried out with chosen performance metrics such as time taken for encryption, time taken for decryption, overall elapsed time and time taken for data retrieval are chosen. From the results, it is proved that the proposed ESCP performs better than that of the other existing methods.

REFERENCES

[1] M. Ali , S. Khan , A. Vasilakos , Security in cloud computing: Opportunities and challenges, Inf. Sci. 305 (2015) 357–383.

[2] R. Aliev , W. Pedrycz , B. Fazlollahi , O. Huseynov , A. Alizadeh , B. Guirimov , Fuzzy logic-based generalized decision theory with imperfect information,Inf. Sci. 189 (2012) 18–42.

[3] N. Cao , C. Wang , M. Li , K. Ren , W. Lou , Privacy-preserving multi-keyword ranked search over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 25 (1) (2014) 222–233 .

[4] D. Chadwick , K. Fatema , A privacy preserving authorisation system for the cloud, J. Comput. Syst. Sci. 78 (5) (2012) 1359–1373 .

[5] C. Chen , C. Zhang , Data-intensive applications, challenges, techniques and technologies: A survey on big data, Inf. Sci. 275 (2014) 314–347.

[6] K. Costa , L. Pereira , R. Nakamura , C. Pereira , J. Papa , A. Falcão , A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks, Inf. Sci. 294 (2015) 95–108 .

[7] L. Darrell, Unlimited cloud storage at amazon.com, inc on black friday, Url = http://www.bidnessetc.com/58232-unlimited-cloud-storage-at-amazoncomincon-black-friday.

[8] Y. Ding , Y. Hu , K. Hao , L. Cheng , MPSICA: An intelligent routing recovery scheme for heterogeneous wireless sensor networks, Inf. Sci. 308 (2015)49–60 .

[9] K. Gai , Z. Du , M. Qiu , H. Zhao , Efficiency-aware workload optimizations of heterogenous cloud computing for capacity planning in financial industry,in: The 2nd IEEE International Conference on Cyber Security and Cloud Computing, IEEE, New York, USA, 2015, pp. 1–6 .

[10] K. Gai , L. Qiu , M. Chen , H. Zhao , M. Qiu , SA-EAST: Security-aware efficient data transmission for ITS in mobile heterogeneous cloud computing, ACMTrans. Embedded Comput. Syst. 1 (2016) 99.

[11] K. Gai , L. Qiu , H. Zhao , M. Qiu , Cost-aware multimedia data allocation for heterogeneous memory using genetic algorithm in cloud computing, IEEETrans. Cloud Comput. 1 (2016) 99.

[12] K. Gai , M. Qiu , B. Thuraisingham , L. Tao , Proactive attribute-based secure data schema for mobile cloud in financial industry, in: The IEEE International Symposium on Big Data Security on Cloud, IEEE 17th International Conference on High Performance Computing and Communications, New York, USA, 2015, pp. 1332–1337.

[13] K. Gai , M. Qiu , H. Zhao , W. Dai , Anti-counterfeit schema using monte carlo simulation for e-commerce in cloud systems, in: The 2nd IEEE International Conference on Cyber Security and Cloud Computing, IEEE, New York, USA, 2015, pp. 74–79.

[14] D. Howley, Is microsoft's onedrive the best cloud storage service?, Url = https://www.yahoo.com/tech/microsoft- kills-unlimited- onedrive- accounts- 1759 27221.html.

[15] M. Li , S. Yu , Y. Zheng , K. Ren , W. Lou , Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst. 24 (1) (2013) 131–143.

[16] Q. Liu , G. Wang , J. Wu , Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inf. Sci. 258 (2014) 355–370 .

[17] A. Parakh , S. Kak , Online data storage using implicit security, Inf. Sci. 179 (19) (2009) 3323–3331.

[18] W. Pedrycz , Allocation of information granularity in optimization and decision-making models: Towards building the foundations of granular computing, Eur. J. Oper. Res. 232 (1) (2014) 137–145.

[19] T. Plantard , W. Susilo , Z. Zhang , Fully homomorphic encryption using hidden ideal lattice, IEEE Trans. Inf. Forensics Secur. 8 (12) (2013) 2127–2137.

[20] M. Qiu , K. Gai , B. Thuraisingham , L. Tao , H. Zhao , Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Gener. Comput. Syst. (2016).

[21] C. Wang , S. Chow , Q. Wang , K. Ren , W. Lou , Privacy-preserving public auditing for secure cloud storage, IEEE Trans. Comput. 62 (2) (2013) 362–375.

[22] L. Wei , H. Zhu , Z. Cao , X. Dong , W. Jia , Y. Chen , A. Vasilakos , Security and privacy for storage and computation in cloud computing, Inf. Sci. 258 (2014) 371–386.

[23] S. Yoon , K. Kim , J. Hong , S. Kim , S. Park , A community-based sampling method using DPL for online social networks, Inf. Sci. 306 (2015) 53–69.

[24] A Anusha Priya, R Gunasundari, Securing Data on the Cloud Server by the User Authentication and Data Security Techniques, 2017, International Journal of Computer Applications, Volume 165, Issue 4.

[25] S.Yasmin, A.Anusha Priya, Decentralized Entrance power with Secret Endorsement of data Stored in Clouds, 2015/8, International Journal of Innovative research in Computer and Communication Engineering, Volume 3, Issue 8, Pages 7279-7284.

[26] V.Yamuna, A.Anusha Priya, Efficient and Secure Data Storage in Cloud Computing RSA and DSE Function, 2015/7, International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Issue 7, Pages 6758-6763.

[27] A Anusha Priya, A Mohanapriya, An Effective Scrutiny of Static and Dynamic Load Balancing In Cloud, August 2016, International Journal of Emerging Technology in Computer Science & Electronics, Volume 23 Issue 4, Pages – 27 -30.

[28] A.S.Syed Navaz, P.Jayalakshmi, N.Asha. 2015. Optimization of Real-Time Video Over 3G Wireless Networks" September. International Journal of Applied Engineering Research. 10(18): 39724-39730.

[29] A.S.Syed Fiaz, N.Asha, D.Sumathi and A.S.Syed Navaz. 2016. Data Visualization: Enhancing Big Data More Adaptable and Valuable. International Journal of Applied Engineering Research. 11(4): 2801-2804.

[30] A.S.Syed Navaz & Dr.G.M.Kadhar Nawaz. 2016. Flow Based Layer Selection Algorithm for Data Collection in Tree Structure Wireless Sensor Networks. International Journal of Applied Engineering Research. 11(5): 3359-3363.

[31] A.S.Syed Navaz and Dr. G.M. Kadhar Nawaz. 2016. Layer Orient Time Domain Density Estimation Technique Based Channel Assignment in Tree Structure Wireless Sensor Networks for Fast Data Collection. International Journal of Engineering and Technology.8 (3): 1506-1512.

[32] A.S.Syed Navaz, N.Asha & D.Sumathi "Energy Efficient Consumption for Quality Based Sleep Scheduling in Wireless Sensor Networks" March - 2017, ARPN Journal of Engineering and Applied Sciences, Vol No - 12, Issue No - 5, pp.–1494-1498.