I. J. Computer Network and Information Security, **2018, 11, 1-8**
Published Online November 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.11.01

Hybrid KP-ABE Algorithm with Time Bounded Access Control for Cloud Data Security

Bhumika Dahat
School of Information Technology, UTD RGPV
E-mail: deepbhumi2821@gmail.com

Dr. Nischol Mishra and Prof. Santosh Sahu
UTD, RGPV Bhopal 462021, India
E-mail: {nishchol@rgtu.net, santoshsahu@rgtu.net}

Received: 14 July 2018; Accepted: 07 October 2018; Published: 08 November 2018

Abstract—Cloud computing presents a vast area for distributed computing where integrated data centres provide resources for immense and scalable distribution of confidential data. Conceptually, cloud applications being offered, information security and its confidentiality become a vital issue to the cloud. So, as to craft certain security of data at cloud data stowage a design and execution of an algorithmic rule to boost cloud security is planned. With an concept, where the planned algorithmic rule integrates option of three completely different existing algorithms and named RAD cryptography algorithm with most novel and attractive conception of Attribute based encryption (ABE) so as to manage, control access and file sharing management in cloud with its special attribute computing properties. During this analysis, a secure file sharing scheme supported attribute is given. In this Research, during this analysis, work data is encrypted using Hybrid attribute based algorithm i.e. RAD Algorithm which proves its proficiency and effectiveness with respect to security level. If any user wants to access the encrypted information where some authentication credentials also are created based on cipher-text, then it has to evidence itself by providing authentication credentials. Consequently, the planned algorithm offers enriched security along with it diminishes time complexity during encryption and decryption technique for data file.

Index Terms—Cloud computing, Data confidentiality, Data Security, ABE, KP-ABE, Time specification and Access control.

I. Introduction

Cloud computing conception has been visualized as design of consequent generation for data Technology (IT) enterprise. In modern period as surveyed on the Internet, the proposal of cloud computing plan deals with dynamic accessible resources that are facilitated. It permits entrance to distant computing amenities and users solely have to be compelled to buy what they require to use, once they need to use it. However, information that is kept within the cloud, the security of the data, its confidentiality and integrity is that the foremost dispute for a cloud user. Thriving past years of cloud computing field leads to its capability to yield users with on-demand, mobile, dependable, and affordable facilities. Overall services of cloud computing has been used in cases of societal networking sites, web mailing, and online file storage & business applications. Cloud storage services hence, provides several advantages i.e. ease of access at anyplace and anytime, high scalable response, resilience, cost adeptness, and high consistency of the data, etc. Therefore, cloud service area owed to these benefits such that specifically each and every individual favours to assign their private data to the cloud storage services whose security remains in doubt these days. These resources could be quickly provisioned and can be relieved with nominal managerial power or service provider interaction.

There are some fundamental challenges for storing delicate information on the cloud servers like Security and privacy of data, its scalability, its confidentiality & integrity and fine grained access control. These considerations have been proved under certain conditions using various techniques by researchers with finite modifications in it. Therefore, data sharing over the cloud servers are highly accessible but has not remained secured, as the cloud service providers can’t be trusted for long. So, the cloud data security issue becomes a huge task to be surmount over the cloud computing are which can be commendably executed with bright techniques of cryptography.

II. Literature Review

Authors in [1] proposed an enhanced version of the classical model of ABE i.e. KP-ABE Scheme that overpower the drawbacks of conventional model of ABE. Exploring KP-ABE when an access structure is linked with certain key whereas set of user attributes is related to cipher-text, then possibly decryption of the cipher-text undergoes when attribute sets of data satisfies the access policy linked to that cipher-text. The KP-ABE is suitable technique for providing the fine grained access control & confidentiality to data system where it can proficiently identify the area for accession of data system, for operation and execution of data over various parts of that system. In [2], Authors have enriched the KP-ABE scheme by adapting Time Specific Encryption technique [5] and proxy re-encryption in proficient manner and they also used the method of adaptable CP-ABE scheme. Adaptable KP-ABE with time interval scheme provides an actual amplification for supervising the task to restrict time interval for decryption. Thus, in [4] authors improved CP-ABE scheme by adaptability of proxy re-encryption scheme for an efficient solution of heavy computation where the re-encryption method of data is entrusted to the cloud as a proxy trusted and it becomes an entrance for the data transformation.

However, in [6,10] authors have expressed effective outsourcing method for decryption of KP-ABE cipher-text and ABE chosen cipher-text security and in [7,11,12] predefined outsourcing scheme has been enhanced with check ability mechanism and verifying the decryption process of the schemes and outsourced data security has also been proved by the authors. Therefore authors in [3] explained the improved version of outsourcing CP-ABE scheme by providing well-organized verification mechanism where they had used blinding algorithm for the decrement of number of exponential setups in the encryption to a constant. Thus, they have assured the check ability for reassurance of the accuracy of their scheme.

Authors in [17] had reviewed and made evaluation with comparison of two significant security techniques i.e. Cryptography and steganography. In [19] Authors in their theory presented novel Secure Transmission of data through DNA cryptographic system using Symmetric encryption algorithm by using two step security encryption algorithm. According to [18], authors have analysed the techniques summing up the classical encryption algorithm procedures with DNA encryption process and clarified how it can be applicable in real world while facing certain challenges. They have summarized DNA computing with each and every conventional cryptographic encryption algorithm. In [26], they proposed a hybrid structure based on Public key cryptography mixing it with DNA cryptography and Digital Signature concept. They further defined the two key pair uses for encryption and decryption algorithm and respectively signature. Thus in [25], the Authors have represented an integrated method to enrich the Symmetric Key Cryptography by using the robust feature of DNA computation in which a novel procedure to twofold the key generation for encryption and decryption process has been introduced.

III. Problem Formulation

In Cloud computing region, the fundamental difficulties are related to cloud data security, data confidentiality, privacy preservation and data backup storage into cloud. As cloud computing facilitates enhances features of security infrastructure where essentially cloud can store immense amount of information and expressively run infinite applications using various security methods but there are huge risks of escaping data from cloud servers during sharing and transmission of data. Therefore, in previous literatures they proved security of their schemas but the techniques are much time consuming and possess inflexible complexities. Consequently, to overpower the problems related to data confidentiality, security and its integrity with fine grained access control of outsourced information and enlighten issues of complexity and time control cloud based cryptographic approach is intended and jumbled up to acquire and ensure superior security of cloud data.

IV. Proposed Methodology

In the proposed methodology, a unique hybrid technique is represented by using integration of Public key Encryption (KP-ABE, RSA), Symmetric key cryptography (AES-256 algorithm) and DNA (algorithm) cryptography. The proposed model explains about the enrichment of data security, its confidentiality & its integrity by time bounded access control which is used to reduce the conflicts of the system during sharing and transmitting delicate data on cloud. Below flowchart of the model describes about how the overall work is implemented for the security of the subtle data over cloud storage. For presenting its security, transmission of data and its sharing here is shown between these users a) data owner and b) data user and c) cloud service provider and d) a proxy server.

A. *Flowchart of Proposed Model*

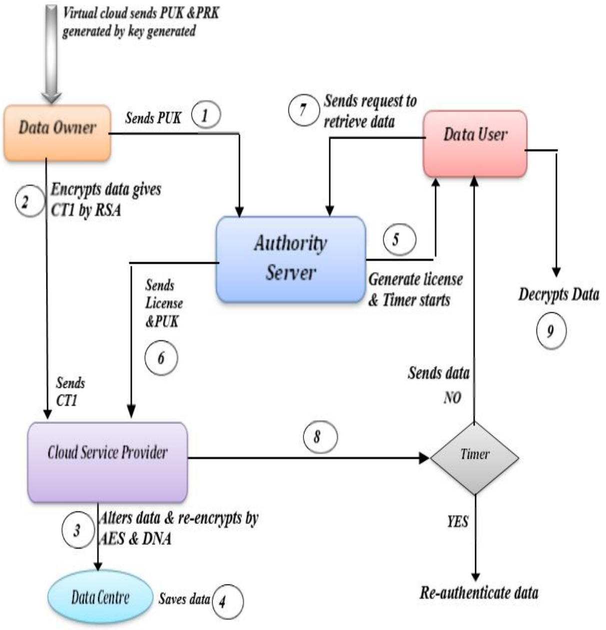
Virtual cloud sends PUK &PRK generated by key generated
Data Owner
Sends PUK
1
7
Sends request to retrieve data
Data User
2
Encrypts data gives CT1 by RSA
Authority Server
5
Generate license & Timer starts
Sends License &PUK
6
Decrypts Data
9
Sends CT1
Sends data
NO
Cloud Service Provider
8
Timer
3
Alters data & re-encrypts by AES & DNA
YES
Data Centre
Saves data
4
Re-authenticate data

Fig.1. Flowchart of Proposed Scheme

According to Fig:1 the steps of flowchart are as follows:

Step (1): Key Generator into Cloud server – CS generates keys in cloud environment and it distributes PUK (public key) and PRK (private key) to cloud users and only PUK to Data owner.

Step (2): Data Owner --Then data owner by his PRK generates SK (secret key) with RSA algorithm and encipher it and transfers the encrypted data CT1 to CSP.

Step (3): Cloud Service Provider -- CSP thus alters the enciphered cipher-text, re-encrypts it into another cipher CT2 by combining AES algorithm and DNA algorithm into final cipher-text CT3 forming a complicated message.

Step (4): Data Centre –Then, the data send by the data owner to the CSP is saved into Data centre.

Step (5), (6): Authority Server (Third Party) —Hence, Authority Server generates the license for data user and after generation of license he sends it to CSP with PUK and then timer starts running.

Step (7): Data User –Thereafter, Data user sends a request for retrieval of data from authority server and unless until he gets permission to retrieve by satisfying his authentication, end user cannot decrypt it.

Step (8), (9): CSP and Timer Expires --When the data user credentials are satisfied i.e. after authentication time specific licence is provided to the end user for accessing data files of owner, i.e. CSP provides encrypted data to the data end user and it generates two conditions; if Timers gives NO condition then data end user has authenticated himself as an authorised user and has time to decrypt data in that interval of time and if Timers YES condition comes, then it seems that user had not decrypted the data in a certain time interval and data is self-destructed.

B. Algorithm of Proposed Work (Amalgam RAD Algorithm)

(Notations: n = integers (big no.), e = encryption of a function, d = decryption of a function, ϕ = function of n (integers), $\prod$= (threshold time, ta<$\prod$<tb),

M= plaintext, C1′ =Encrypted Cipher-text by RSA, C2′= encrypted cipher-text by AES, C3′= encrypted cipher-text by DNA], λ = attribute parameters

(*U_Id= user ID, O_Id= Owner ID, F_Id= File Id, Date, R_ID= receiver Id****)****, U1 =data owner, U2 =data end user, CS = Cloud Server, CSP = cloud service provider, PRK= Private Key, PUK= Public Key, SK = Secret Key, AS= Authority server.)*

(1) SETUP PHASE: *CS generates PUK & PRK into a cloud environment.*

(2) KEY GENERATION PHASE:

(i) Generated PUK = {X, A_1, A_2, A_3.....An}
(ii) Generated PRK = {x, a1, a2, a3... a_n}

- *Select two prime numbers M and N such that M ≠ N and determine*

$$\sigma= M*N \tag{1}$$

- *Calculate ϕ= (M-1)(N-1)* (2)
- *Find PUK and PRK such that*

$$PUK = PRK^{-1}[mod\ \phi] \tag{3}$$

- *Where PRK = gcf [ϕ, PRK] =1* (4)
{1< PRK< ϕ}
- *SK = (λ, PRK)* (5)

{□ λ = attribute parameters (U_Id, O_Id, F_Id, Date)}

(3) ENCRYPTION PHASE:

Step-(I) *Cipher (byte Msg, byte C1′)*

```
    begin {
            $C1' = Msg^{PRK}\ mod\ \sigma$          (6)
    end
  }
```

Step-(II) //C1′ and C2′ are byte arrays which are assumed to be input data and output ciphered data respectively.

// position [] is a 2-dimensional array holding bytes in 8 rows and 8 columns.

//roundSeckey[] is an array holding the SK for algorithm round.

//RoundSecKey(), Sub_Bytes(), Shift_Rows(), and Mix_Columns() are functions representing the discrete alterations. And its Inv. those are converse functions.)

```
Cipher (byte C1′, int SK, byte C2′, key-array roundSeckey(N+1))
        begin byte position [32]; position= C1′;
  {
  Add RoundSecKey(position, roundSeckey[0]);
   for l = 1 to N-1 stepsize 1
  do Sub_Bytes(position);
  Shift_Rows (position);
  Mix_Columns (position);
  Add RoundSecKey (position, roundSeckey[l]);
  end for
  Sub_Bytes (position);
  Shift_Rows (position);
  Add RoundSecKey (position, roundSeckey[N]);
  C2′ = position;
```

```
    end
    }
```

```
Step-(III)  Cipher (byte C2′, byte C3′)
        state = C2′;
        begin {
            convert ASCII code(state);
            convert binary code(state);
            pairing(state);
            DNA digital coding(state);
            DNA sequencing(state);
            C3′ = DNA sequencing(state);
        end
        }
```

(4) AUTHENTICATION PHASE:

```
    U2 (λ2) ⇒ AS   {λ2= Data attributes (O_Id, F_Id, R_Id)
    if (λ2 = = λ1) satisfies {λ1 =Attributes (U_Id, F_Id, date)
    then go to decryption phases;
    else
    exit.
```

(5) DECRYPTION PHASE:

```
Step-(I)    Decipher (byte C3′, byte C2′)
    State = C3′;
    begin {
            DNA op.sequencing(state)
{op.sequencing applied for opposite DNA sequencing}
            DNA_digital.decoding(state);
            convert binary code(state);
            Convert ASCII(state);
            C2′ = convert byte(state);
      end
    }
```

```
Step-(II)   Decipher (byte C2′, byte C1′, round Seckey
            (N+1))
    begin byte position [32] ; position = C2′
    {
      Inv.Add RoundSecKey(position, roundSeckey[N]);
        for l = 1 to N-1 stepsize 1
        do Inv_Shift_Row (position);
          Inv_Sub_Bytes (position);
          Inv_Mix_Column(position);
        end for
          Add RoundSecKey (position, roundSeckey[l]);
          Inv_Shift_Rows (position);
          Inv_Sub_Bytes (position);
          Inv Add RoundSecKey (position,
          roundSeckey[0]);
          C1′= position;
        end
    }
```

```
Step-(III)  Decipher (byte C1′, Msg)
            begin {
                    $Msg = C1'^{PUK}\ mod\ \sigma;$          (7)
            end
          }
```

```
Step-(IV)   If d [C2′, C1′, Msg] < ∏ {decryption
            satisfies threshold time interval ta < ∏ < tb}
          then download Msg;
          else;
          Msg destroyed,
          exit.
```

V. IMPLMENTATION AND PERFORMANCE ANALYSIS

First of all, the cloud atmosphere is created using cloudsim. The proposed work has simulated in the cloud environment with two data center having two data user. Here, one of the users is the data owner i.e. whose data file is stored at the cloud server and other data user is the receiver who desires to access the data file of the owner.

After generation of cloud surroundings, the key generator of cloud server generates public and private key and provide it to both data owner and end user. But, as such data owner is responsible for further encryption of data owner sends only his public key to the cloud authority server (CAS) for further decryption process.

Simultaneously, when data owner wants to save data file at the data centre then he firstly generates the secret key by Algorithm-step-I (Encryption) of RAD algorithm using User Id/ Owner Id, File Id and Date as attributes of the file.

After secret key generation, the cloud service provider encrypts the data file using the generated secret key using step-II and step-III of RAD algorithm. After encryption CSP (Cloud Service Provider) handover the encrypted data to cloud data center for further uploading the file.

Whenever any cloud end user needs to access the data file of the data owner, then it has to authenticate himself by providing authentication credentials in a given time interval i.e. File Id, Receiver’s Id and Owner’s Id.

If all the authentication credentials matches, then only the data user is provided authentication rights to access the data file stored at data center in encrypted form. Otherwise, data end user is declared as unauthorized user.

After authentication of the user, CAS provides the public key of data owner and secret key to the data user so as to retrieve file from the data server/ data center.

Therefore, when a user gets decryption keys a timestamp is started for the decryption of data for end data user to access or retrieve the data file from the data center. If the data is decrypted with specific license in the predefined time interval then data could be accessed by end user otherwise the data is destroyed and the end user has to reauthenticate himself.

VI. EVALUATION OF EXECUTION TIME

In Table:1, the execution time analysis has been computed of the proposed method that explains the Key

Generation time analysis, Encryption time analysis and Decryption time analysis of various different types ofdata file size. Therefore it has been evaluated that as the file size increases the key generation time, encryption time and decryption time increases gradually.

Table 1. Computational Time Analysis

S. No.	File Size	Key Generation Time (in ms)	Encryption Time(in ms)	Decryption Time (in ms)
1.	10MB	4	24	4
2.	15MB	5	25	4
3.	20MB	5	25	4
4.	60MB	6	26	10
5.	120MB	8	37	12

Then in Fig: 2 the key generation time has been examined graphically where from 10MB to 15MB the graph take a speed gradually but remain constant between 15MB to 20MB and then again gradually increases accordingly with the file size.

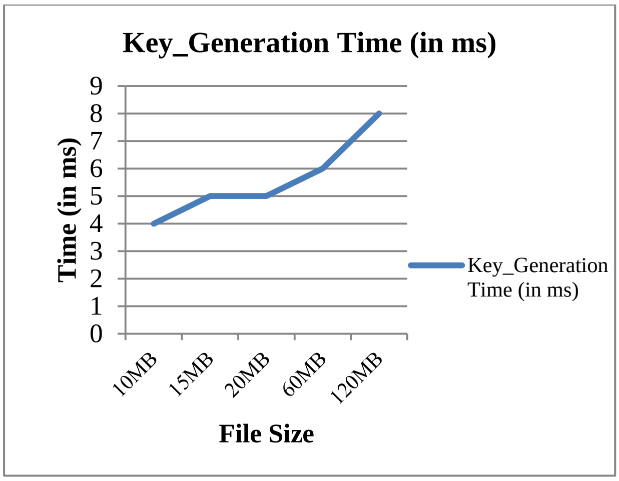

Fig.2. Key Generation Time Analysis

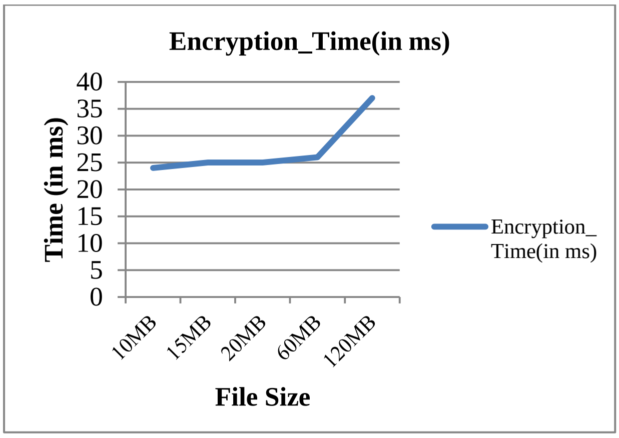

Fig.3. Encryption Time Analysis

Therefore in Fig: 3 the encryption time has been evaluated. Here, initially the from 10MB to 15MB there minor increment and from 15MB to 20MB the graph remains constant and slightly increases to 60 MB and then suddenly increases up to 120 MB according to file size.

Hence, Fig:4 shows decryption time analysis where the graph remains constant from 10MB to 20 MB and gradually increases from 20MB to 120 MB.

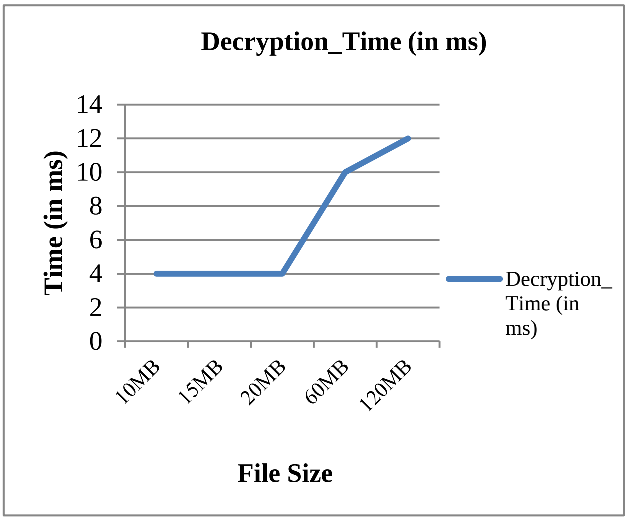

Fig.4. Decryption Time Analysis

A. *Comparative Analysis*

The Presented proposed model is therefore equated with previous paper [30] and by analysing it is found that our proposed arrangement is quite less time consuming, reliable, cost effective and proficient as compared for encryption time and decryption time of various sorts of data sizes ranges from 100KB to 50MB (i.e. 100KB, 500KB, 1MB, 2MB, 5MB, 10MB and 50MB). As the consumed time period for both encryption phase and decryption phase is calculated by following Formula:

Time consumption = Execution stop time – Execution start time

Thus, in Table:2 the comparative analysis for proposed and existing times of encryption and decryption has been shown in mili-seconds. Hence, after observing the comparison of both existing and proposed technique, it can be assessed that as for encryption, time fluctuates i.e. decreases and increases gradually as increase in the file size and for the decryption, time increases gradually as the data size increases.

And, in Fig:5 and Fig:6 the observations of encryption and decryption time of proposed method has been compared with existing system [30] in the same files size range from 100 KB to 50 MB which shows the huge difference.

Table 2. Comparative Analysis of Proposed Method

S. No	File Size	Encryption Time (in ms)		Decryption Time (in ms)	
		Proposed	Existing [30]	Proposed	Existing [30]
1.	100 KB	31	21	1	16
2.	500 KB	31	73	1	58
3.	1 MB	30	150	15	122
4.	2 MB	31	173	15	151
5.	5 MB	31	210	15	193
6.	10 MB	24	421	16	394
7.	50 MB	26	1220	16	1110

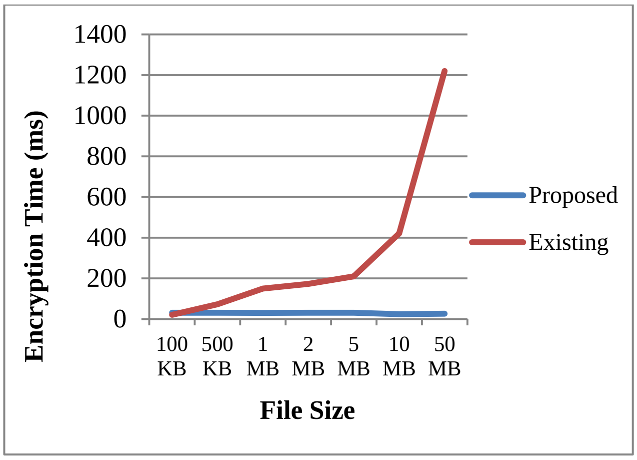

Fig.5. Encryption Time Comparison

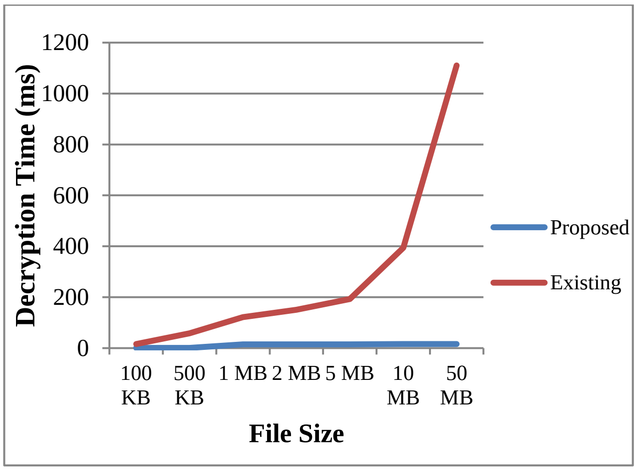

Fig.6. Decryption Time Comparison

VII. Conclusion

Exploration of presented work is concentrated on cloud information security at cloud end. To create solid data protection of cloud data repository at cloud end, the fortified architecture is designed that secures and shield the data using encryption/decryption algorithm where the proposed algorithm is a hybrid encryption algorithm that uses the concept of CSP (Cloud service Provider) and CAS (Cloud Authority Server). The technique Key policy attribute based encryption is used with hybrid technique of RSA, AES and DNA cryptography algorithm which is executed in the planned methodology for the access of encrypted cloud data which created an well-organized system in terms of execution time and security as compared to the existing methods of cloud data retrieval.

Therefore, fruitful results are produced by the implementation of proposed methodology. Tested outcomes indicate that the projected idea is affordable; its improved potency in terms of execution time, security and providing confidentiality of cloud data at cloud end is quite rational.

Also, the re-encrypting of data three times before sharing and transmitting to cloud end users provides a tough key that could hardly be cracked for its accession. This technique is applied differently in this method with time that reduces the encryption and decryption time as compared which create uniqueness in it. This effort of research also uses the concept of authentication of the user. The planned method provides a sheltered framework for confidentiality of text information at cloud data stowage which will be beneficial in an exceedingly range of applications at cloud end. Simplicity and confidentiality are the inclusions in the advantage of the planned methodology.

Therefore, outcome analysis illustrates that this technique takes less computational time and hence overall cost is less. Although, in terms of security and retrieval rate and computational time the well-organized technique has been implemented here shows novelty, but further enrichments may be trialled for the communication overhead and latency that may appears during the encrypted data retrieval.

Acknowledgement

I thank to my respected Guide and Co-guide with all professors who directed me thoroughly in right path for this paper. This work was supported by School of Information Technology University of Teaching Dept. RGPV Bhopal.

References

[1] Goyal V, Pandey O, Sahai A, Waters B (2006) "*Attribute-based encryption for fine-grained access control of encrypted data*". In: Proceedings of the 13th ACM conference on computer and communications security.

[2] Ma J, Lai J, Deng R H, Ding X (2016) "Adaptable key-policy attribute based encryption with time interval."

[3] Jing L, Xiong L, Licheng W ,Debiao H, Haseeb A, Xinxin N(2017) "Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption".

[4] Lai J, Deng RH, Yang Y, Weng J (2013) "*Adaptable cipher-text policy attribute-based encryption*". In: Pairing-based cryptography— pairing 2013. Springer.

[5] Paterson KG, Quaglia EA (2010) "*Time-specific encryption"*. In: Garay JA, De Prisco R (eds) Security and cryptography for networks. Springer, Berlin.

[6] Green M, Hohenberger S, Waters B (2011) "Outsourcing the decryption of ABE cipher text".

[7] Huang X, Li J, Li J (2014) "*Securely outsourcing attribute-based encryption with check ability"*. Transactions on Parallel and Distributed Systems, Vol. 25, No. 8.

[8] Xhafa F, Wang J, Chen X (2014)" An efficient PHR service system supporting fuzzy keyword search and fine-grained access control".

[9] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu(2008)" Expressive Key-Policy Attribute-Based Encryption with Constant-Size Cipher text".

[10] Chao Li, Bo Lang and Jinmiao Wang(2014) "Outsourced KP-ABE with chosen cipher-text security".

[11] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on outsourced attribute-based encryption," in Computer Security–ESORICS 2013. Springer, 2013.

[12] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," Information Forensics and Security, IEEE Transactions (2013).

[13] Rivest RL, Shamir A, Wagner D A (1996) "Time-lock puzzles and timed release- cryptography.

[14] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, (2007).

[15] Goyal, V., Jain, A., Pandey, O., Sahai, A. "Bounded Ciphertext Policy Attribute Based Encryption". In: Aceto, L., Damg˚ard, I. Goldberg, L.A., Ing´olfsd´ottir, A., Walukiewicz, I. (eds.) ICALP 2008.

[16] Tysowski, P.K., Hasan, M.A.: Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds. Technical Report 13, Centre for Applied Cryptographic Research (CACR), University of Waterloo (2013).

[17] "*A Survey On Recent Approaches Combining Cryptography And Steganography*" David C. Wayld et al: Computer Science & Information Technology (CS & IT), SIP, CST, ARIA, NLP – 2017 pp. 63– 74.

[18] Anurag Roy, Ashoke Nath *"DNA Encryption Algorithm –Scopes And Challenges in Symmetric Key Cryptography*" International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 3 (November 2016).

[19] Bonny B. Raj, J. Frank Vijay, T. Mahalakshmi "*Secure Data Transfer through DNA Cryptography using Symmetric Algorithm*" International Journal of Computer Applications (0975 – 8887) Volume 133 – No.2, January 2016.

[20] Gritti, C., Susilo, W., Plantard, T. & Win, K. (2015). *Privacy-preserving encryption scheme using DNA parentage test.* Theoretical Computer Science,

[21] Anupriya Aggarwal & Praveen Kanth "*Secure Data Transmission Using DNA Encryption*" IOSR Journal of Computer Engineering (IOSR-JCE) Volume 16, Issue 2, Ver. II (Mar-Apr. 2014).

[22] A Fatma E. Ibrahim. M. I. Moussa, H. M. Abdalkader "*Symmetric Encryption Algorithm based on DNA Computing*" International Journal of Computer Applications (Volume 97 No.16, July 2014.

[23] Jaspal Kaur Saini and Harsh K Verma "*A Hybrid Approach for Image Security by Combining Encryption and Steganography*" Proceedings of IEEE 2013 Second International Conference on Image Information Processing.

[24] Ronak Doshi, Pratik Jain, Lalit Gupta "*Steganography and its Applications in Security*" International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638.

[25] Bibhash Roy, Gautam Rakshit, Pratim Singha, Atanu Majumder, Debabrata Datta "*An improved Symmetric key cryptography with DNA based strong cipher*" IEEE Device and Communication (ICDeCom) 2011 International Conference.

[26] Lai X J, Lu M X, Qin L, et al."*Asymmetric encryption and signature method with DNA technology.*" Science China Press and Springer-Verlag Berlin Heidelberg 2010.

[27] Adleman L. "Molecular computation of solutions to combinatorial problems". Science, 1994.

[28] Dan Boneh, Cristopher Dunworth, and Richard Lipton. "*Breaking DES Using a Molecular Computer"*. Technical Report CS-TR-489-95, Department of Computer Science, Princeton University, USA, 1995.

[29] Ashish Gehani, Thomas LaBean, and John Reif "DNA-Based Cryptography" A preliminary version appears in DIMACS DNA Based Computers V, American Mathematical Society, 2000.

[30] Bokhari et.al, Shallal et.al "*Evaluation of Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computing"* International Journal of Computer Applications volume -166, no.4 May -2017.

Authors' Profile

Bhumika Dahat was born in Bhopal in 1992 and she has completed her Bachelor of Engineering in Electrical Engineering and now perusing Masters of Technology in Information Technology from UIT, RGPV Bhopal, India. Her research Interest is Cloud Cryptographic themes, cloud computing, Information Security.

Dr. Nishchol Mishra has completed his Bachelor's Degree and Masters Degree in Computer science and he has awarded in P.hd with specialization in computer science. He is currently an Associate professor in the Department of Information technology (M.E, M.TECH) in SOIT UTD, RGPV University, Bhopal, India and he has 15 years' experience for teaching.

Prof. Santosh Sahu has completed his Bachelor's Degree in Information Technology and gained his Masters in Technology (M.Tech) with the specialization in Information Technology. He has worked for 8 years as a lecturer in different colleges and recently he is an assistant professor in the IT department (M.E, M.TECH) in SOIT, UTD, RGPV University, Bhopal, India.

How to cite this paper: Bhumika Dahat, Nischol Mishra, Santosh Sahu,"Hybrid KP-ABE Algorithm with Time Bounded Access Control for Cloud Data Security", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.11, pp.1-8, 2018.DOI: 10.5815/ijcnis.2018.11.01