European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 02, 2020

Identity Based Adaptive Key Encryption for Data Security in Cloud Environment

Mrs. T. Sujithra [1], Dr. M. Sumathi [2], Dr. M. Ramakrishnan [3]
[1] Research Scholar, Madurai Kamaraj University, Maduai – 21, Sujithra.thangam@gmail.com
[2] Associate Professor and Head, Department of Computer Science, Sri Meenakshi Govt, Arts College for Women, Madurai-21, Sumathivasagam@gmail.com
[3] Professor and Head, Department of Computer Applications, Madurai Kamaraj University, Madurai - 21 Ramkrishod@gmail.com

ABSTRACT

Cloud computing shares resources and services; adore dispersive data, code and hardware platforms, through net and virtualization technologies. Because of the difficult structure and co-share feature of cloud computing. Encryption and authentication are this key techniques for the protection of large knowledge throughout cloud computing. Encryption and decoding are unremarkably applied ways for knowledge security. Time has forever competed animperativetask in communication. Data will turn intoineffective once a finickyposition; sensitive knowledge might not be free before a particular time. Identity-based systems have a characteristic downside operating. This limitation could also be overcome by together with a time element within the identity. Through this manuscript, we have a tendency to novel cryptographic technique referred to as Time Stamp encryption (TSE) that addresses this downside. In our planned work introduce a brand new paradigm utilize time parameters that embody cryptography formula offers as high secured, powerful validation and scale back the time quality for encryption mechanism.

Key words: Time Stamp, Time Stamp Encryption, Adaptive Key

1. Introduction

Cloud computing shares resources and services, resembling dispersive info, computer code and hardware platforms, through web and virtualization technologies, that provides dynamic distortion service to users following market demand. Users acquire resource from service provider through terminal, particularly mobile terminal. the normal challenge of personal information security eventually becomes a lot of vital, thanks to the sophisticated structure and co-share feature of cloud computing. Encoding and authentication are this key techniques for the safety of huge information throughout cloud computing. the info encrypting ways are therefore emerged by the growing demand of information security.

Data encryption and decryption are normally applied ways for information security. Data encryption is the process of forming cipher text from the plain text by encryption algorithmic rule and key. The reverse process is known as decryption. Encryption technique is assessed into symmetric Cryptography Algorithms and asymmetric Cryptography Algorithms. Symmetric encryption means users encrypt and decrypt information by exploitation constant password. The password may be a command, dominant the encrypting and decrypting processes. Algorithmic rule may be a set of rules, crucial a way to encrypt and decrypt. Therefore, symmetric encryption isn't safe by itself. asymmetric encrypting methodology overcomes the challenge of key transfer, by applying completely different keys throughout encrypting and decrypting.

However, the general public key combination cannot manage the valid amount of physical key. The disappearance of entity makes the existence of physical key become wastes. Hence, the valid amount for the physical key's applied to affect the keys in step with given rules. Key management is that the key challenge for the safety of cloud computing. The communication of each parties in self-authenticated method doesn't believe the third party for key generation and transmission, that not solely solves the key security management, however additionally reduces the energy consumption for transmittal keys throughout cloud computing. Self-authentication is outlined as an authentication and encryption method, within which the third party (e.g. CA center) isn't needed within the method of key exchange. Each sender and receiver will verify the corresponding public keys supported the general public identity provided by the counter party and verify the non-public signature of the counter party. Additionally, a user will verify the general public key in step with the public identity provided by the other users, and use the general public key for information encrypting and transmittal, to appreciate sharing and transmittal information between specific users. Throughout these processes, the

third party is excluded from effort the general public key, which reduces the network resource consumption and improves the safety of information encryption and authorization.

Time has perpetually via a crucial position in sharing information. Information will become ineffective once a specifiedreason, responsive information wouldn't be free earlier than a selected instance, otherwise they tend to may need towards modify right to use the information for less than a restricted amount of your time. During this context, having the ability to specify throughout what amount a cipher text will be decrypted by a recipient may be a helpful as well as attention-grabbing possessions.

Identity-based methods have a distinguishingdrawback in process. Assume Alice and Bob are client of such a method. In view of the fact that the knowledge required toward search out Alice's public key's fully indomitable by Alice's ID and therefore the master public key, it's impracticable to retract Alice's ID and issue new identification while not moreover (a) ever-changing Alice's ID; or (b) varying the master public key and reissue non-public keys to everyone or a few users, also for Bob.

This restriction could also be conqueringthroughas one with a time factor (for example this month) within the identity. During this paper, we tend to new cryptographic prehistoric known as Time Stamp encryption (TSE) that addresses this drawback. In our planned work introduce a replacement paradigm utilize time parameters that embrace cryptography algorithmic rule provides as high secured, powerful validation and cut back the time quality for data encryption mechanism.

II. Related Work

Time Specific encryption [4] will useTime Instant Key (TIK) which means that every amount of time which broadcast by Time Server. The dispatcher of information will denote any period time throughout encoding progression; the recipient is able to rewrite and recover the information providing that time factor TIK with the intention of exchange to a time therein time period. They have a tendency to expand basic TSE to the public key and ID based settings, wherever recipient are to boot preparedamong non-public key and either public key or identity, and wherever cryptography currently needs the employment of the non-public key still as an acceptable TIK. They introduced safety and secure methods for the plain, public key and ID based settings.

Adaptive ID Secure revocable Identity based encryption [5], describe an IBE theme endued with an identical and uniformlywell-organized revocation methodsince within the BGK system whereas attainsafety measureswithin the effective adaptive ID wisdom, wherever adversaries opt for the target identity within the challenge section. It emphasizes that, though comparatively free, the lessening is complexity within the range of salable queries. Our building uses identical dual tree arrangement and applies the same revocation technique.

Time-bound key-aggregate encoding for cloud storage [6], shall suggest a timebound enter combination encoding theme for cloud storage, beside the consequences of a fewassessment still as accuracy and safetyinvestigation, they need created to prove the prevalence of our novel theme over connected mechanism. Not solely can the theme take the load of uphold the attribute-based keys rotten the client, however it'll additionally give acceptablediscretion

Self-Authenticated methodology with Timestamp [7], the current invention relates to an authentication methodology for digital communication, particularly a self-authenticated methodology with timestamp, and associated knowledge encrypting and decrypting strategies, mutual self-authenticated of communicators, and renewal of self-authentication.

We have a tendency to propose ID based mostly adaptive key encoding in cloud surroundings to validate participant authentication in secured cloud storage. Each Id based mostly algorithmic rule should have characteristic drawback thanks to generate non-public key for receiving user. To over calm the matter, we have a tendency to introduce adaptive key to incorporate time stamp details admire time parameters to validate the participant users.

The manuscript organizes as Time Stamp adaptive Key Techniques, Work flow of time Stamp, adaptive Key encryption, Results, Performance Analysis and Conclusion.

III. Time Stamp Adaptive Key Technique

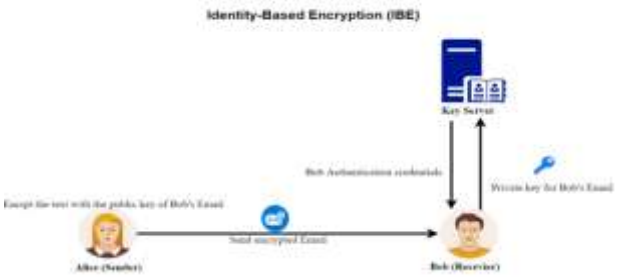
Identity-based scheme permit somefestivity to come up with a public key as of a notable identity assessment such as an ASCIIsequence. A trustworthy third party, referred to as the private key generator (PKG), produce the equivalent private keys. To function, the PKG is first issue a master public key, and keep hold of the equivalent master private key. Given the master public key,

any festivity will calculate a public key similar in the direction of the identity ID by join the master public key with the uniqueness worth. To get a resultant private key, the festivity approved to use the identity ID contacts the PKG,which uses the master private key to come up with the private key for identity ID

As a result, festivity might encrypt messages with rebuff previous distribution of keys flanked by individual participants. This is often extraordinarily helpful in cases wherever presharing of legitimate keys is difficult or impracticable thanks to technologicalfetters. However, to decrypt or sign messages, the approved user should acquire the suitable private key from the PKG.[3]

A caution of this method toward is that the PKG should exist extremely trustworthy, because it becompetent of produce any user's private key and should thus decrypt messages while not approval. As a result of any user's private key may be generated through the employment of the third party's secret, this technique has intrinsic key escrow. Identity-based cryptograph mechanisms consist of public key encryption in which a sender will produce a public key from a prominenteffectivemark such as an email ID, and a believable third-party server computeequivalent private key from the general public key. On this situation, there's no had to be obliged to hand out public keys proceeding to switch over encrypted message. The dispatcher will simply use the typical symbol of the recipient to arrive up with a public key and encrypt the message. The recipient will produce the equivalent private key with the help of the convictionworthy third party server the private key generator (PKG).

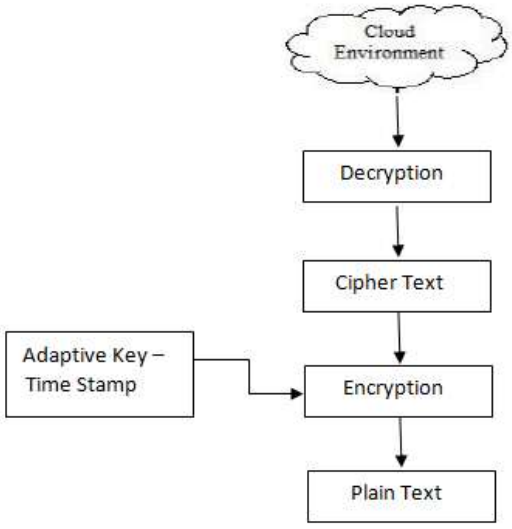
To manage this cryptographpremise, the PKG first bring out a master public key, and preserve the equivalent master private key. Given the master public key, any party will compute a public key related to an identity by merge the master public key with some distinguished identity worth.To get a equivalent private key, the proprietor of the identity won't to produce the common public key acquaintances the PKG, that employ its master private key to arrive up with the equivalent private key.



IV. Problem Statement

ID based mechanism havetypical issues in function. Assume Alice and Bob are client of such a scheme. In view of the fact that the messages are needed to locate Alice's public key is entirelydogged by Alice's ID and the master public key, it is not probable to retract Alice's identification and problem new identificationdevoid of either (a) altering Alice's ID or (b) altering the master public key and re-producing private keys to every clients, as well as Bob.[2]

This restriction may be conquering by together with a time element (for example the current month) in the ID.



The Time component has constantlyplays significant role in communication. Information can turn intouseless after a specific timeline. Perceptiveinformationmight not be released earlier than specified periods of time. Sometimes we may want to allowinteract to the information for barely an inadequateinterlude of time. From above conditions, the time period for the activation of decryption plays a vital role in communication. This helps to the recipient for specifying the timelines.

The author proposed novel new mechanism in this research article, the author introduced new cryptograph scheme is known as Time Stamp Encryption (TSE) that will beconcentrate on this issue. Furtherin particularly, the author believes an arrangement that will bebelief the Time Server (TS). TS presents the Time Instant Key (TIK) kt at every time unit or \tick" of its clock, t, where 0 <= t <= T-1. This TIK is obtainable to everyuser, and the author absolutely assumes that it includes the narrative of t. A dispatcher can denotesome interval [t0; t1], where t0<= t1, when encrypting a plaintext m to form a ciphertext c. In Plain TSE, the author want to carry out the attribute in which c can only be decrypted by a recipient to improve m if the recipient knows tenure of an TIK kt for some t with t € [t0; t1]. [1]

Observewith the intention of the author can able toput effectinto the attribute that the recipient can merely decrypt for the period of decryption time interval (DTI) [t0; t1], in view of the fact that a recipient can get for all timean appropriate TIK and next utilize it when they want. Accomplish this impression must be completeby means ofconviction hardware, for example. However, theauthor discuss below about Time Server Encryption TSE havea number ofinterestingrelevanceutilize its important attribute that a recipient must attain a appropriate TIK prior competent to perform decryption.

V. Work Flow of Time Stamp

In this Context, the author will introduce a novel methodology of time stamp adaptive key encryption mechanism,in begin, the author will describe the building block of proposed mechanism, and then they will describe the particulars of each phase in proposedmechanism. To start with, the members ofproposed scheme consist with the cloud storage environment (CSE), the data owner, and the user [8]. The three members[9]perform as describe follows:

Cloud Storage Environment (CSE): The CSEwants to accumulate the cipher text and admitnecessitiesdrive from the user. CSE also has the capability of re-encrypting the time stampof cipher text.

Data owner: The data owner desires to encrypt the cipher text and locate anequivalent class to everyportion of it. The data owner also produces a time stampof adaptive key for the user[9].

User: The user desires to propel a prerequisite to the data owner in arrange to get hold of his or her key, and nextpropel another prerequisite to CSE to acquire the re-encrypted cipher text. The user afterward employs the time stamp adaptive key specified by the data owner to decrypt the ciphertext conventional [9].

The author was to assign λ as the entirely suitable time for the user. This manner, while the user promise for a time period [t 1, t 2], the variables T, λ , x , y , t , t 1, and t 2 convince the following depiction,

$$t_1 + x = t = t_2 - y,\ x + y = \lambda,\ t_2 - t_1 = \lambda \leq T$$

VI. Adaptive Key Encryption Algorithm
SystemSetup:

The author needs to setup the proposed Adaptive Key Encryption System[5,1,4] in the following ways,
Let $g_i = g^{a^i} \in G$ for i = 1, …, n , n + 2, …, 2n .
Next calculate T sets of public parameters B = {B 1, B 2, …, B T },
Where every set B k consists k + 1 keys.
Every k + 1 keys as totally, they are called D k ,u = α + a u b k − u , ∀ u ∈ [0, k], ∀ k ∈ [0, t], where u and k are the past time and the total time, correspondingly.
Further, the author have the system, parameters param = (B , g , g 1, …, g n , g n + 2, …, g 2n , e k g , g α).
Perceivewith the aim of the association of B , B k , and D k ,u can be explained as follows:
Suppose that T = 4; there exist B = {B 1, B 2, B 3, B 4}, and every B k consists k + 1 keys:[4]

$$B_1 = \{D_{1,0},\ D_{1,1}\} = \{\alpha + a^0 b^1,\ \alpha + a^1 b^0\}$$
$$B_2 = \{D_{2,0},\ D_{2,1},\ D_{2,2}\} = \{\alpha + a^0 b^2,\ \alpha + a^1 b^1,\ \alpha + a^0 b^2\}$$
$$B_3 = \{D_{3,0},\ D_{3,1},\ D_{3,2},\ D_{3,3}\}$$
$$= \{\alpha + a^0 b^3,\ \alpha + a^1 b^2,\ \alpha + a^2 b^1, \alpha + a^3 b^0\}$$
$$B_4 = \{D_{4,0},\ D_{4,1},\ D_{4,2},\ D_{4,3},\ D_{4,4}\}$$
$$= \{\alpha + a^0 b^4,\ \alpha + a^1 b^3,\ \alpha + a^2 b^2,\ \alpha + a^3 b^1,\ \alpha + a^4 b^0\}$$

KeyGen:

Select γ ∈R Z p ; nextcalculate the public key pk = υ = g γ and master secret key mk = γ

Encrypt:

The data owner encrypts the message and selects a equivalent class to each ciphertext. in favor of a message m i ∈ G T and an index i ∈ {1, …, n }, randomly choose β ∈ Z p , and calculate the ciphertext C i = (c 1, c 2, c 3, c 4) = (g αβ , g β , (υg i)β , m i ê (g 1, g n)β).

Extract:

The data owner produces a time stamp adaptive key for the user. For the set S of indices j s, the adaptive key can be calculatedby,

$$K_S = e_k g^{\gamma} a'^{t_1} b^{z - t_2} \prod_{j \in S} g^{\gamma}_{n+1-j}$$

Subsequent tocalculate K S , the data owner propel it back to the user during a secure channel. by way of this key, the user can decrypt the cipher text preferred.

Re-encryption:

Aheadin receipt of the obligation from the user, CSP produce a new time-bound ciphertext for the user. CSP wishes to re-encrypt the stored cipher text. CSP calculates

$$c_4' = c_4 / \hat{e}\left(g \cdot \prod_{j \in S, j \neq i} g^{\gamma}_{n+1-j+i}, c_2\right)^{a'^{t_1} b^{z-t_1} e_k} \cdot \hat{e}\left(g \prod_{j \in S, j \neq i} g^{\gamma}_{n+1-j+i}, c_1\right)^{a'^{t_1} b^{z-t_2} e_k}$$

After that proceeds $C_i' = (c_1,\ c_2,\ c_3, c_4')$ to the user as re-encrypted ciphertext.

Decrypt:

If the user decrypts the ciphertext in suitable time, the user can use K S to decrypt the re-encrypted cipher text by calculating.

$$m_t = c_4' \cdot \hat{e}\left(K_S \prod_{j \in S, j \neq i} g_{n+1-j+i}, c_2\right)^{D_{k,u}} \hat{e}\ (g_{n+1}, c_2)^{D_{k,u}}\ \hat{e}\left(\prod_{j \in S} g_{n+1-j},\ c_3\right)^{\nu_{k,u}} \cdot \hat{e}(g_{n+1},\ c_2)$$

Earlier than calculating m i , the user wants to locate the equivalent B k in B to get D k ,u $= \alpha + a\ u\ b\ k - u$ in tidy to decrypt the ciphertext.

Results

The adaptive key encryption utilizes the time stamp parameters which include with encryption techniques. To achieve high data security we can use combined Time Stamp Adaptive Key with cryptographic technique for validate the participants. It restrictsunconstitutional users to interact the data in Cloud Storage Environment.

VII. Performance Analysis

In this section, we shall compare our proposed Adaptive Key Time Stamp Encryption with the following parameters, Validation, Time Parameters, Re-Encryption. Validation means that author validate the participant not only with personal credential but validate and verify with the time parameters. Other parameters are such that Re-Encryption utilize in our proposed algorithm for data security.

Our proposed algorithm is compare with Adaptive Key Encryption and Time bound key aggregation algorithm. Adaptive key Encryption which uses personal credential for generating the key and Time based key generated by Time bound key aggregation algorithm.

Comparison of Performance Analysis

Algorithms	Validation	Time Parameters	Re-Encryption
Adaptive key time stamp encryption	Yes	Yes	Yes
Adaptive key Encryption	Yes	No	Yes
Time bound key aggregation	No	Yes	Yes

VIII. Conclusion

The cloud Computing may be a promising technology to safe guard the helpful and wind from unauthorized users in our planned work victimization adaptive key time stamp cryptography used for additional accuracy and high information security. In our proposed work introduce a brand new paradigm utilize time parameters that embrace cryptography algorithm provides as high secured, powerful validation and cut back the time complexness for data encryption mechanism. the mix of this time stamp based algorithm to store the secured information and restricted access from unauthorized users in cloud environment. so by implementing time stamp based adaptive key algorithm in cloud environment that turn cloud information may be secured.

References

1. Shamir. Identity-based cryptosystems and signature schemes, in Advances in Cryptology — Crypto ’84, Lecture Notes in Computer Science 196 (1984), Springer, 47–53.
2. https://en.wikipedia.org/wiki/ID-based_cryptography
3. Bishoi, TANMOY KUMAR, RAMKRISHNA GHOSH, and TANMOY SINHA ROY. "An algorithm on text based security in modern cryptography." J ComputNetwWirel Mobile Commun 5.1 (2015).
4. https://securityboulevard.com/2019/09/identity-based-cryptography/
5. Time-specifcencryptionkenneth g. Paterson and elizabeth a. Quaglia information security group, royal holloway, university of london,
6. Lee, Cheng-Chi, Chun-Ta Li, Shih-Ting Chiu, and Shun-Der Chen. "Time-bound key aggregate encryption for cloud storage : Time bound key-aggregate encryption for cloud storage" , Security and Communication Networks, 2016.
7. Raghava, N. S., and Ashish Kumar."Image encryption using henon chaotic map with byte sequence." International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) 3.5 (2013): 11-18.
8. Adaptive-ID Secure Revocable Identity-Based Encryption. BenoîtLibert, Damien Vergnaud. Topics in cryptology - CT-RSA 2009, 2009, San Francisco, United States.
9. To Enhance the Data Security in Cloud Computing Using Multimodal Biometric System World Wide Journal of Multidiciplinary Research and Development 2017 P. Selvarani, N. Malarvizhi

10. Bhar, Sreya. "Encryption Key Generation by Using Modified Hand-Geometry Based Cryptosystem to Secure SMS in Android." International Journal of Computer Science and Engineering (IJCSE) 4.5 (2015): 17-26.
11. Eike Kiltz, Gregory Neven: Identity-Based Signatures. Identity-Based Cryptography 2009: 31-44.
12. Swamy, Srinadh, Pavan Kumar, and VASU DEV. "IMPR OVED AUTHENTICATION TECHNIQUE TO PROTEC T WEB APPLICATIONS." International Journal of Computer Science and Engineering (IJCSE) ISSN (P): 2278-9960.
13. ShejiNishoni, A. Aldo Tenis. "Secure Communication With Data Analysis and Auditing Using Bilinear Key Aggregate Cryptosystem in Cloud Computing" , Materials Today: Proceedings, 2020.
14. Kenneth G. Paterson. "Time-Specific Encryption" , Lecture Notes in Computer Science, 2010.