ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

Renewable Keyword for Data Store Application in Secure Cloud Storage Using Enhanced Hyper Elliptical Curve Cryptography

Jeyaprabha.C [1] , Dr.S.Karthigai Selvi [2]

Department of Computer Science, Sakthi College of Arts and Science for Women Oddanchatram, TN, India [1]

Department of Computer Science, Sakthi College of Arts and Science for Women Oddanchatram, TN, India [2]

ABSTRACT: Cloud services are used by many organizations and it has captured a major segment of the competitive market today. The green, or eco-friendly, aspect of the cloud is one of the most multifaceted advantages of cloud computing. Temporary keyword search on confidential data in a cloud environment is the main focus of this research. The cloud providers are not fully trusted. So, it is necessary to outsource data in the encrypted form. In the attribute-based keyword search (ABKS) schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation. These search tokens can be used to extract all the cipher texts which are produced at any time and contain the corresponding keyword. We introduce a new cryptographic primitive called key-policy attribute-based temporary keyword search (KPABTKS) which provide this property. In this method, initially the authentication of the user is verified. Once the authentication of the user is verified successfully dual encryption is performed on the cloud stored files using ElGamal cryptosystem and Hybrid Elliptical Curve Cryptography (HECC). The aim for using the proposed system is for analysis of security which can be enhanced through the technique of sharing many keys amongst the two parties. The proposed technique performance is evaluated in reference with environmental protection, storage cost, computation cost and execution time and is implemented in JAVA. The experimental results show the efficacy of the system as it utilizes only less time for both encryption and decryption of sensitive data.

KEYWORDS: Environmental benefits, Cloud services, Key-policy attribute-based temporary keyword search, Hybrid Elliptical Curve Cryptography, Decisional Bilinear Diffie-Hellman algorithm(DBDH)

I. INTRODUCTION

Cloud Computing evolved through the distributed software architectures scalability and extensibility (Khan and Al-Yasiri 2016). According to the National Institute of Standards and Technology (NIST) definition, “the cloud computing is a model for enabling convenient, resource pooling, ubiquitous, ondemand access which can be easily delivered” (Singh et al. 2016b). It is transforming ways to hardware and software design and procurements activities. Services without cost, elasticity of resources, accessibility through internet etc. are some of the benefits that cloud technology offers. With all of the recent buzz about cloud computing, companies have learned that by switching to a public cloud, they can gain flexibility and scalability while simultaneously cutting costs. But what they may not realize is that the cloud not only benefits their workplace, but also, the environment. Managing and processing data on a local server greatly increases carbon emissions. Almost all enterprises (big or small) are aiming towards enhancing businesses and tie-ups with other enterprises through the use of cloud technology (Vurukonda and Rao 2016); SaaS, PaaS, Iaas and Private, Public, and Hybrid are the service and deployment models respectively. One of the key reasons why it faces

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

more security problems is due to high availability to end users. Public key encryption with keyword search (PEKS) is a cryptographic primitive which was first introduced by Boneh et al. to facilitate searching on the encrypted data. In PEKS, each data owner who knows the public key of the intended data user generates a searchable ciphertext by means of his/her public key, and outsources it to the cloud. Then, the data user extracts a search token related to an arbitrary keyword by using his/her secret key, and issues it to the cloud. The cloud service provider (CSP) runs the search operation by using the received search token on behalf of the data user to find the relevant results to the intended keywords.

Introduced the notion of attribute-based key-word search (ABKS) to allow a data owner to control the access of data users for searching on his/her outsourced encrypted data. They used attribute-based encryption (ABE) [3] to construct a searchable cryptographic primitive in the multi-sender/multi-receiver model. In their work, the legitimate data users can enlist the cloud to run the search operation on behalf of them without requiring any interaction with the data owner. In a secure ABKS scheme, a data owner cannot obtain any information about the keywords which the data users intend to look for. However, in all of the PEKS and ABKS schemes, once the cloud receives a valid search token related to a certain keyword, the cloud can investigate the keyword's presence in the past and any future ciphertext. So, if the adversary realizes the corresponding keyword of the target search token, then she will be able to get some information about the next documents which will be outsourced to the cloud. Therefore, it will be more secure to limit the time period in which the search token can be used.

Motivated by this problem, Abdalla et al. [4] introduced the notion of public key encryption with temporary keyword search (PETKS) which restricts the validation of the token to a certain time period. They applied anonymous identity-based encryption [5] in their generic scheme. In addition, Yu et al. [6] proposed another public key searchable encryption in the context of temporary keyword search. Despite the good features of their schemes, these schemes do not provide the facility for data owners to enforce their intended access policy. In this paper, we propose a novel notion of Key-Policy Attribute-Based Temporary Keyword Search (KP-ABTKS). In KP-ABTKS schemes, the data owner generates a searchable ciphertext related to a keyword and the time of encrypting according to an intended access control policy, and outsources it to the cloud. After that, each authorized data user selects an arbitrary time interval and generates a search token for the intended keyword to find the ciphertext. Then, he/she sends the generated token to the cloud to run the search operation. By receiving the token, the cloud looks for the documents contain the intended keyword. The search result on a ciphertext is positive, if (i) the data user's attributes satisfies the access control policy, (ii) the time interval of the search token encompasses the time of encrypting, and (iii) the search token and the ciphertext are related to the same keyword. To show that the proposed notion can be realized, we also propose a concrete instantiation for this new cryptographic primitive based on bilinear map.

II. LITERATURE SURVEY

To assess the environmental impact of cloud computing, Microsoft engaged with Accenture—a leading technology, consulting and outsourcing company— and WSP Environment & Energy—a global consultancy dedicated to environmental and sustainability issues—to compare the energy use and carbon footprint of Microsoft cloud offerings for businesses with corresponding Microsoft on-premise deployments. The analysis focused on three of Microsoft's mainstream business applications— Microsoft Exchange®, Microsoft SharePoint® and Microsoft Dynamics® CRM. Each application is available both as an on-premise version and as cloudbased equivalent. 2 The team compared the environmental impact of cloud- based vs. on-premise IT delivery on a per-user basis and considered three different deployment sizes—small (100 users), medium (1,000 users) and large (10,000 users). The study found that, for large deployments, Microsoft's cloud solutions can reduce energy use and carbon emissions by more than 30 percent when compared to their corresponding Microsoft business applications installed on-premise. The benefits are even more impressive for small deployments: Energy use and emissions can be reduced by more than 90 percent with a shared cloud service. Several key factors enable cloud computing to lower energy use and carbon emissions from IT:

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

- Dynamic Provisioning: Reducing wasted computing resources through better matching of server capacity with actual demand.
- Multi-Tenancy: Flattening relative peak loads by serving large numbers of organizations and users on shared infrastructure.
- Server Utilization: Operating servers at higher utilization rates.
- Data Center Efficiency: Utilizing advanced data center infrastructure designs that reduce power loss through improved cooling, power conditioning, etc.

Though large organizations can lower energy use and emissions by addressing some of these factors in their own data centers, providers of public cloud infrastructure are best positioned to reduce the environmental impact of IT because of their scale. By moving applications to cloud services offered by Microsoft or other providers, IT decision- makers can take advantage of highly efficient cloud infrastructure, effectively "outsourcing" their IT efficiency investments while helping their company achieve its sustainability goals. Beyond the commonly cited benefits of cloud computing— such as cost savings and increased agility—cloud computing has the potential to significantly reduce the carbon footprint of many business applications.

RDA method proposed by Sookhak et al. (2016) was based on features of algebraic signature. The cost of computation and communication incurred are minimum. Divide and Conquer Table (DCT) presented by them could sustain dynamic data operation and applicable even for data storage in a comprehensive way. The proposed RDA techniques have proven to be more enhanced in terms of security and efficiency with least cost of computation and communication on the server and the auditor.

The cryptography approach proposed by Rohini et al. (2017) impedes cloud service operators to get to the partial data directly. In this approach, file is divided and subsequently data is stored separately. In order to find whether the data packets require to be divided for reducing operation time, an alternative approach was developed.
Zhang et al. (2016) proposed a method named match-then-decrypt. As the name indicates, an additional phase called as a matching phase was introduced prior to the decryption phase. That technique worked by computing special components in cipher texts, which were used to perform the test that if the attribute private key matched the hidden access policy in cipher texts without decryption. The purpose of this process was to expedite the process of decryption by facilitating the pairing aggregation. An anonymous ABE construction was proposed and a security enhanced extension was then obtained. During the process of attribute matching, the cost involved for computation was less than decryption operation.

III. PROPOSED WORK

To analyzed and classified existing works on cloud data management, focusing on multiple users to retrieve the data from cloud store its major requirements, which help to retrieve the data from cloud store without any conflicts. In propose our end-to-end solution to support multiple users to access these applications in cloud environments. The proposed concrete scheme is designed based on bilinear pairing. In the proposed key-policy attribute-based temporary keyword search (KP-ABTKS), each user is identified with an access control policy. The data owner selects an attribute set, and runs the encryption algorithm with regard to it. Today, the world of core business processes has a lot of dependency on Cloud computing. But it is very vulnerable to attacks since it is internet based.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

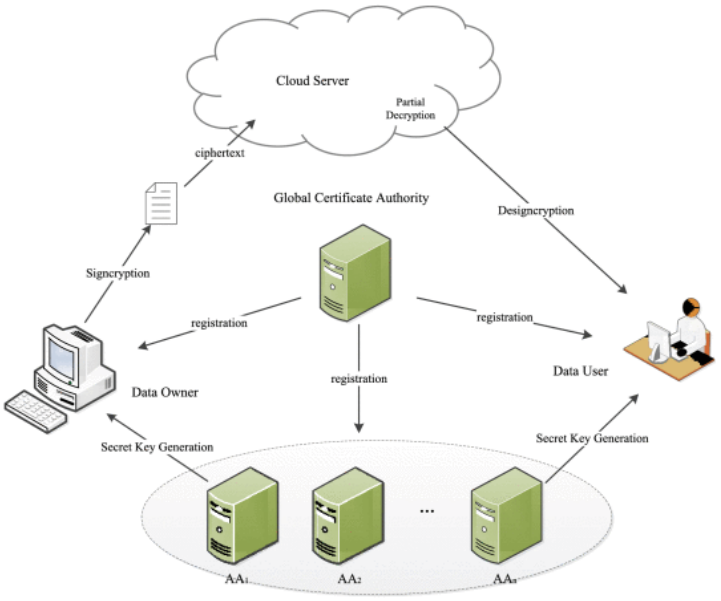

Fig 1: The semantic structure of recommended technique

Therefore the issue of security is of paramount concern. That is why Cloud security has attracted attention of the research community. With ABTKS, data owner will first encrypt the index that is searchable and for double encryption the Hyper Elliptical Curve Cryptography is utilized. The explicit formula for point doubling and point addition in HECC is subjected to modification in hyper elliptic curve. The suggested technique overall semantic architecture is shown in Fig. 1. Proposed virtual data stores to execute complex queries (including joins) across NoSQL and relational data stores. For this purpose, we defined a unifying data model able to describe the heterogeneous data models of data stores. It is used by the user to express his second chance and by the virtual data store to process it. The search result on a ciphertext is positive, if (i) the data user's attributes satisfies the access control policy, (ii) the time interval of the search token encompasses the time of encrypting, and (iii) the search token and the ciphertext are related to the same keyword. To show that the proposed notion can be realized, we also propose a concrete instantiation for this new cryptographic primitive based on bilinear map.

Advantages:

- The proposed KP-ABTKS scheme consists of five algorithms, Setup, KeyGen, Enc, TokenGen, and Search.
- Here generate the renewable keyword for user request.
- Data fetching time is too short.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

IV. SYSTEM IMPLEMENTATION

ARCHITECTURE DIAGRAM:

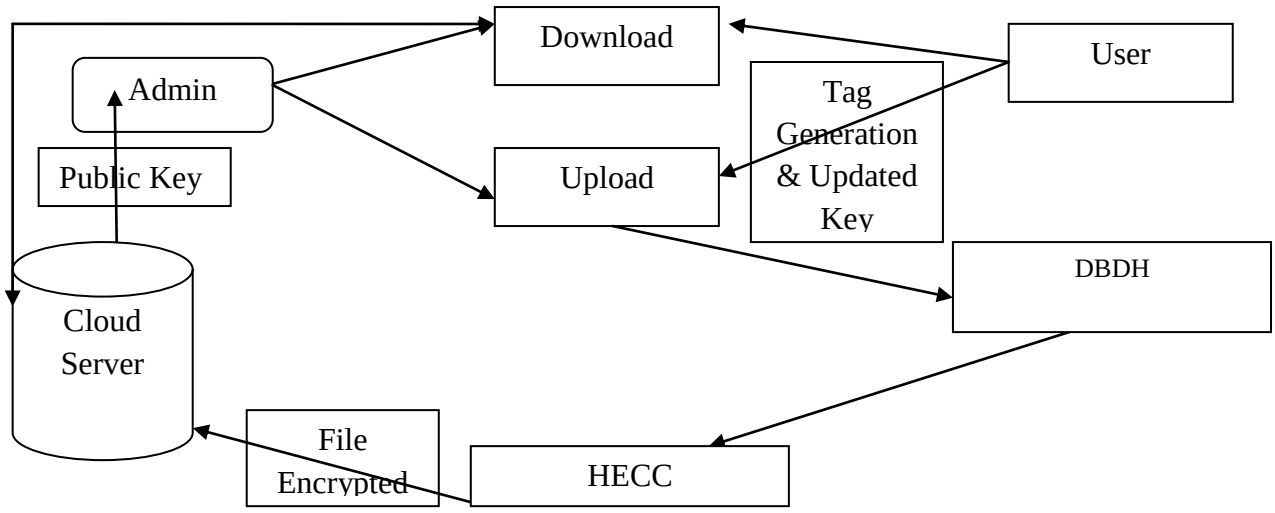

Fig 2: Working Process

4.1 HYBRID ELLIPTICAL CURVE CRYPTOGRAPHY (HECC):

The proposed HECC message is coded with the symmetric code and the key over the coded message is encrypted using the asymmetric coding algorithm. Fig2: showsThe creator will now take the data key and will decode it using the asymmetric coding algorithm to that the recipient's public key. The operation forms a key Block. But the advantage of this is thought it is highly compute intensive the size of the data key which we are taking is very small thus the complete process will be done in just a fraction of second. The creator will collect the data block and the key which was stored as a block into a file and transmits the file to the recipient The new Hybrid ECC (HECC) has two stages of operation which are explained in the following sub sections:

4.1.1 STAGE 1

At first the originator and the recipient of the data must both agree on the parameters for ECC, that is, the domain parameters of the scheme. The field of domain in ECC is defined by 'p' in the prime case and the pair of 'c' and 'd' in the binary case. The elliptic curve is defined by the constants 'a' and 'b' used in its defining equation. The elliptical curve will now be a plane curve which is simple and spread over finite field. It consists of points which satisfy the equation

$$y^3=x^3+ax=b \qquad (4.1)$$

along with a distinguished point at infinity, denoted .

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

4.1.2 STAGE 2

The Generator G will be defining the Monogenerous group that is generated by the single element. There are several logarithm based protocols that are available, which will restore the (Zp)x with the elliptical curve. Here we are choosing Elliptic curve Diffie –Hellman key agreement scheme based on Diffie Hellman scheme is being used. 31 For cryptographic application G, which is the smallest non-negative number n so that nG=∞, which in most cases is prime. Since n is the size of a subgroup of E(Fp) from Lagrange's theorem it can be shown that the number h is an integer. The h is expressed in eqn

$$H= |E(F_p)|/n \qquad (4.2)$$

In cryptographic applications this number h, which is the cofactor, must be small and preferably h should be 1. Unless and until there is assurance that the parameters are generated by the trusted party they need to be validated before we use them The generation of domain parameters is not usually done by each participant as this process involves computing the number of points on a curve. This process is compute intensive, time-consuming and troublesome to implement. There are few domain parameters which are already proposed by the standard bodies for several common field sizes to overcome this reason [65]. These domain parameters which are termed as named curves which can be the NIST (National Institute of Standards and Technology) curve. The above mentioned algorithms will generate the curve based on the respective fields. But if any user wants to create their own parameters than there are several strategies that are available and mentioned below which can be used to generate the curve with the required set of points on the field: Firstly, The user can select the random curve and then apply a general pointcounting algorithm like Schoof's algorithm or Schoof–Elkies–Atkin algorithm, Select a random curve in a family of curves like the Koblitz curve can be used or Select the number of points required and then generate a curve with this number.

The projected phenomenon can be compared to a finite-field cryptography (e.g., DSA) that will need 3072-bit public keys and 256-bit private keys, and integer factorization cryptography (e.g., RSA) which requires a 3072-bit values of n, Hence, even if the public key is large, the private key which can be small will be used for encryption. With the smaller key size less computation and faster processing will be achieved. Especially smaller processors are present.

User Generation:

User generation module is used to generate the admin and client login pages. Admin can able to upload the n - num of to the cloud with help mCP-ABE; at that same time that client can also view the received data with the help of ABT. In this module to create a n-num of users without any interruption.

Data Encryption & Decryption:

In this paper, we propose a new scheme for attribute revocation in CP-ABE called mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE). Previous CP-ABE systems proposed to use a system where attributes are valid within a specific time frame. However, the drawback of thisapproach is that there is no way to revoke an attribute before the expiration date. In our scheme the secret key is divided into two shares, one share for the mediator and the other for the user. To decrypt the data, the user must contact the mediator to receive a decryption token. The mediator keeps an attribute revocation list (ARL) and refuses to issue the decryption token for revoked at-tributes. Without the token, the user cannot decrypt the ciphertext, therefore the attribute is implicitly revoked.

Key Policy Construction:

In ABT (Attribute based token), user secret key components consist of a single personalized key and multiple attribute keys. The personalized key is uniquely determined for each user to prevent collusion attack among users with different attributes. The proposed key generation protocol is composed of the personal key generation followed by the

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

attribute key generation protocols. It exploits arithmetic secure 2PC protocol to eliminate the key escrow problem such that none of the authorities can determine the whole key components of users individually. Personal Key Generation: The central authority and each local authority are involved in the following protocol.When a sender wants to deliver its confidential data, hedefines the tree access structure over the universe of attributes, encrypts the data under to enforce attribute-based access control on the data, and stores it into the storage node. Then a user receives the ciphertext from the storage node, the user decrypts the ciphertext with its secret key. The algorithm performs in a recursive way. We first define a recursive algorithm that takes as inputs a ciphertext , a private key , which is associated with a set of attributes, and a node from the tree.

Renewable Key Updation:

When a user comes to hold or download the data time expired means, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively. The key update procedure is launched by sending a request for some attribute group from a user who wants to hold or download the file to the corresponding authority. On receipt of the membership change request for some attribute groups, it notices the storage node of the event. Without loss of generality, suppose there is any membership change in (e.g., a user comes to hold or download a file using renewable keyword).

Cloud Storage Server

Our scheme is the first to allow privacy-preserving public auditing for regenerating code-based cloud storage. The coefficients are masked by a PRF (Pseudorandom Function) during the Setup phase to avoid leakage of the original data. Cloud storage to be a collection of n storage servers, data file F is encoded and stored redundantly across these servers. Then F can be retrieved by connecting to any *k*-out-of-*n* servers, which is termed the (mCP-ABE) -property.
A TPA, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. In this system, the cloud audit server also generates all the tags of the files for the users before uploading to the cloud storage server. The basic goal of PoR model is to achieve proof of retrieve ability. Informally, this property ensures that if an adversary can generate valid integrity proofs of any file F for a non-negligible fraction of challenges, we can construct a PPT machine to extract F with overwhelming probability.

V. CONCLUSION

In this paper, secure storage of data in cloud is offered based on double encryption of ElGamal and HECC algorithms. ElGamal and HECC are utilized in our proposed method for encryption and decryption with some modification to normal process. The use of double encryption enhances data security as the security of sensitive data from unauthorized access is essential requirement of cloud environment. We have utilized Decisional Bilinear Diffie-Hellman algorithm(DBDH) algorithm for integer selection in ElGamal cryptosystem. And for key generation in HECC, we have utilized addition and doubling of point using elliptic curve cryptography. The user secures the input message with ElGamal and HECC cryptosystem algorithms. The proposed method performance analysis is done in regards to storage cost, computation cost and execution time. Results indicate that our proposed data security model is more efficient with regards to storage and computation cost and minimum time than the existing methods.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,”
[2] H. Shacham and B. Waters, “Compact proofs of retrievability,”
[3] K. D. Bowers, A. Juels, and A. Oprea, “Proofs of retrievability: Theory and implementation,”
[4] E.-C. Chang and J. Xu, “Remote integrity check with dishonest storage server,”

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 1, January 2020

[5] T. S. J. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage,"
[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing,"
[7] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds,"
[8] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms of outsourcing modular exponentiations,"
[9] Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage,"
[10] H. Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen, "Towards end-toend secure content storage and delivery with public cloud,"
[11] H. Li, B. Wang, and B. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud,"