REVIEW-FREE DISTRIBUTED STORAGE BY MEANS OF DENIABLE ATTRIBUTE BASED ENCRYPTION

[1]K.V.Anjani, [2]Dr. R. Jegadeesan, [3]V.Sai Sri Mahitha, [4]P.V.Sri Harshini, [5]B.Shiva, [6]N.Anudeep, [7]Dr.D.Srinivas

[3,4,5,6]UG Students, [2,6]Associate Professor-Dept. of Computer Science and Engineering,
[1,2,3,4,5,6]Jyothishmathi Institute of Technology & Science, Karimnagar, India

Abstract: Transformations square measure obligatory to mount the unstoppable stream of amendment. The majority of associations are endeavoring to lessen their registering cost through the methods for virtualization. This interest of decreasing the processing cost has prompted the advancement of Cloud Computing. The most appealing administration/service of cloud computing is Data outsourcing, because of this the information proprietors, who are commonly called as data owners can have any size of information on the cloud server and clients can get to the information from cloud server when required. As servers and information proprietors are clear personalities, the example of information accumulating raises different security challenges. It is hard to decide if the cloud storage providers meet the client's desires for information security. Numerous plans were proposed for keeping up honesty of cloud information yet practically speaking those plans neglect to ensure the information respectability. This structure is exhibited for a cloud storage encryption conspires which empowers cloud storage providers for making the convincing forged/fake client secrets so as to secure client protection. Since coercers can't reveal whenever acquired private details are valid or not.

Index Terms **– Deniable Encryption, Cloud Storage, Security, Coercers, Data outsourcing.**

I. INTRODUCTION:

Cloud computing design has watched a broad move towards its reception and it has turned into another propensity in the data innovation space as it guarantees striking cost decreases and new business potential outcomes to its clients and suppliers. The cloud storage providers are in charge of keeping the data unfilled and open, and the physical condition protected and running. To store the application information from the clients, there are different organizations which purchase or rent the capacity limit from the cloud storage providers. The buyers can stock their related information on the cloud and can even access the information from any point whenever just by associating with the web. This occurs in a cloud storage condition.

The information which has been put away on the cloud is typically encrypted and verified from the access by different clients. The fundamental reason for this encryption and security is because of the client's protection. By considering into record concerning the collaborative property of the cloud information, Attribute-Based Encryption (ABE) is a standout amongst the most acceptable encryption plans for the cloud storage. It is likewise one sort of public key encryption. In this, the cipher-text and the secret key of the client will rely upon attributes. In that way, just when the arrangement of qualities of the client key will be proportionate to the attribute of the cipher text, at that point just the decryption of cipher text would be possible. In this, the cloud storage providers use certain techniques to make convincing fake user secrets. By permitting certain fake user secrets, the outside coercers can just secure fake information from the client's stored cipher text. On the off chance that the coercers trust the secrets they got were genuine, at that point they will be satisfied. The cloud storage providers need not to give any sort of the secrets. Subsequently, the protection for the client's information is saved.

This thought principally originates from an extraordinary sort of encryption plot called deniable encryption. Senders and recipients make strong fake evidence of fake information in the cipher-text with the end goal that the outside coercers will be satisfied. Deniable encryption includes such sort of procedure. This thought is utilized so those, the cloud storage providers can give review free/inspection free storage administrations (services). This plan depends on Waters cipher-text policy-attribute based encryption (CP-ABE) conspires. The Waters plot/scheme is being expanded from prime order bilinear groups to Composite order bilinear groups. It empowers the clients to most likely give the fake secrets that appear to be legitimate to the outside coercers by the subgroup choice issue.

II. LITERATURE SURVEY:

Sahai and Waters presented Attribute-based encryption (ABE) [1], takes into consideration pounded get to control on encrypted information. In its key-policy enhance (the double cipher-text approach situation continues the different way), to encode/encrypt messages under a lot of attributes and private keys are connected with access structures that indicate which cipher-texts the key holder will be permitted to decode/decrypt. In most ABE frameworks (systems), the cipher-text size has added substance development with the quantity of cipher-text attributes and the main realized which is the only known exception supports restricted types of fasces arrangements. The work about the attribute based encryption (ABE) plans taking into account genuinely open access structures and with constant cipher-text size. In the first outcome, cipher-text policy based ABE scheme with O(1)- size cipher-texts for threshold access policies and where private keys stay as short as in past frameworks (systems). In the second outcome, they demonstrated that a specific class of identity based broadcast encryption schemes typically gives monotonic key-policy attribute-based encryption (KP-ABE) frameworks (systems) in the particular set model. The last undertaking is a KP-ABE acknowledgment supporting non-monotonic access structures (i.e., that may contain invalidated attributes) with short cipher-texts. As a moderate advance towards this outcome, they depicted a proficient identity-based cancellation system that, they joined with a specific portrayal of their general monotonic development, offers ascend to the most expressive KP-ABE acknowledgment with constant-size cipher texts. The drawback of the second and third developments (constructions) is that private key shave quadratic size in the quantity of attributes. Then again, they lessen the number of pairing evaluations to a consistent, which gives off an impression of being a unique feature among communicative KP-ABE plans.

An essential plan is utilized that permits a client (a sender or a recipient) to keep his information away from the coercers. The coercers constrain the cloud storage providers to uncover the information of the client data sources and outputs. Since an old encryption plot submits the client to his random inputs, the client is compelled to uncover the true results of all his random inputs (counting the encrypted/decrypted messages and the encryption/decryption keys) but by utilizing deniable encryption we can confine coercers to watch our information. We can make fake information of the client with the end goal that it will persuade the coercer enemy as unique information and the coercer can't discover whether the information is fake or unique. By this the client can hide his unique information from being observed.

An abstract system [2], is created which encases the key properties of bilinear gatherings/groups of composite order that are required to assemble the secure pairing based cryptosystems, and it is disclosed that how to utilize prime-order elliptic curve groups to build bilinear groups with similar properties. In particular, a summed up rendition of the subgroup decision problem is characterized and gives explicit constructions of bilinear gatherings in which the generalized subgroup choice assumption pursues from the choice DiffieHellman supposition, which is the decision linear assumption, as well as related assumptions in prime-order gatherings. In this, the system and prime-order group developments are connected so as to make all the more efficient forms of cryptosystems which at first/initially requires composite-order gatherings. By chance, Boneh Sahai-Waters double crosses following framework; which if formerly known as traitor tracing system, Boneh-GohNissim encryption scheme, and Katz-Sahai-Waters attribute based encryption schemes are considered. A security hypothesis is utilized for the prime-order aggregate instantiation of every framework that utilizes assumptions of comparable complexity to those utilized in the composite-order setting.

As of late [3], the security of tasks occurring over a PC organize turned out to be essential. It is important to ensure such activities against "awful" clients who may attempt to abuse the framework (e.g. steal credit card numbers; execute activities without approval, read individual mail etc.). Numerous cryptographic protocols and plans were intended to take care of issues of this sort. This proposition manages two principal cryptographic tools that are helpful in such settings: generalized secret sharing plans, and key conveyance plans.

Deniable encryption [4], is an important thought that permits a client (a sender or a receiver) to get away from a coercion attempt. Such an enemy approaches the constrained client after transmission compelling him to uncover all his irregular information sources utilized amid encryption or decoding. Since conventional encryption plans submit the client to his irregular sources of information, the client is compelled to uncover the genuine estimations of all his arbitrary information sources (counting the encrypted/decrypted messages and the encryption/decoding keys) which are unquestionable by this coercer utilizing the intercepted cipher text. In this situation, a coercer may compel the client to perform activities against his desire. In this paper they presented a plan for sender deniable public key encryption by which the client can lie about the encrypted message to a coercer and consequently, escape coercion. While the receiver can decode for the genuine message, the sender can open a fake message of his decision to the coercer which when confirmed gives the equivalent cipher-text as the genuine message. Their plans depend on quadratic residuosity of a two-prime modulus. Deniability upgrades to these plans considering the sender's nearby randomness are likewise displayed. The best way to construct a proficient deniable open key encryption from any trapdoor change is explained. These plans require significantly less data transmission; give more grounded deniability and no decoding blunder.

After the execution of the protocol [5], the coercers may drive the clients to uncover the information so client and the cloud provider convey in unreliable channel with the end goal that coercer can't see the information of the client. This is finished by permitting the client and cloud supplier to make inward states which can be seen and decrypted by just those gatherings. Deniable encryption was thusly introduced with permit denying a message trade and hence combating coercion. Contingent upon which groups can be pressured the security level, the avor and the quantity of rounds of the cryptosystem; it is conceivable to prevent a number from claiming thoughts of deniable encryption. It is demonstrated that there does not exist any non-interactive receiver deniable cryptosystem with superior to polynomial security. This additionally demonstrates it is difficult to develop a non-interactive bi-deniable public key encryption conspire with superior to polynomial security. Extraordinarily, an explicit bound relating the security of the plan to how effective the plan is regarding key size is given. The difficulty result sets up a lower bound on the security. As an invalid commitment they permitted developments of deniable public key encryption plans which set up upper limits on the security as far as key length. There is space between lower and upper limits, which leaves the fascinating open issue of completion the tight limits.

Deniable encryption [6], presented in 1997 by Canetti, Dwork, Naor, and Ostrovsky, ensures that the sender or receiver of a secret message can "counterfeit" the message encrypted in a particular cipher message within the sight of a forcing adversary, without the enemy recognizing that he was not given the genuine message. They proposed the first sender-deniable public key encryption framework with a solitary encryption algorithm and negligible detection probability. They portrayed a nonexclusive interactive development dependent on a public key piece encryption plan that has certain properties, and gave two instances of encryption plans with these properties, one dependent on the quadratic residuosity suspicion and the other on trapdoor stages.

This work [7] was done in understanding of working with security and capacity over the distinctive accessible segments. In the current framework, there are different associate issues which are worked in their proposed work AES-256 is very simple and normally accessible for the programmer movement in the event that it wish to break. In this paper they have utilized a standard SHA-2 algorithm for message key generation and for the information encryption, they utilized advanced Bluefish calculation. After this process, they additionally found the proxy server in cloud system. Their proposed work primary idea is to give a high-security approach while dealing with the cloud security approach, as the general methodology either works with the security encryption or hashing data check framework.

A group of associations [8], utilizing encrypted correspondence or putting away information in an encrypted structure may be compelled to demonstrate the comparing plaintext. It might occur because of power from higher specialists like government authorities or from political pioneers. Canetti at el proposed deniable encryption demonstrates that cryptography can be utilized against uncover information: the proprietor of the information may look up to decrypt the information in an obverse way to a harmless plaintext. Also, it is difficult to check if there is another cloud plaintext. The plan of Canetti is incompetent as it is a special scheme and utilizing it demonstrates that there is some obscure message inside. They uncovered that deniable encryption can be implemented diversely with the goal that it doesn't point to profiting deniable encryption. Besides, it is very unambiguous, so it very well may be utilized for both great and malice purposes.

In this work [9], a deniable ABE plot for appropriated storage organizations is depicted. The use of ABE characteristics has been made for ensuring cover data with a fine-grained get the chance to control part and deniable encryption to neutralize outside assessing. This plan relies upon the Waters cipher-text system quality based encryption plot. In this work, they have updated the Waters scheme from prime order bilinear groups to Composite order bilinear groups. By the subgroup decision issue thought, their plan catches clients to have the ability to give fake insider facts that appear apparently to be consistent with outside coercers. In this work, they built a deniable CP-ABE conspire that can make distributed storage organizations secure and inspection free.

Cloud computing provides [10], users with ample computing resources, storage, and bandwidth to meet their computing needs, often at minimal cost. As such services become popular and available to a larger body of users, security mechanisms become an integral part of them. Conventional means for protecting data privacy, such as encryption, can protect communication and stored data from unauthorized access including the service provider itself. Such tools, however, are not sufficient against powerful adversaries who can force users into opening their encrypted content. In this work we introduce the concept of deniable cloud storage that guarantees privacy of data even when one's communication and storage can be opened by an adversary. We show that existing techniques and systems do not adequately solve this problem. We first design the sender-and-receiver deniable public-key encryption scheme that is both practical and is built from standard tools. Furthermore, we treat practical aspects of user collaboration and provide an implementation of a deniable shared file system, DenFS.

Attribute based encryption (ABE) [11], is a dream of public key encryption that enables clients to encrypt and decrypt messages dependent on client attributes. This usefulness includes some major disadvantages. In a typical execution, the extent of the cipher-text is corresponding to the number of attributes related with it and the decoding time is relative to the number of attributes utilized amid decryption. In particular, numerous ABE executions require one matching task for every attribute utilized amid decryption. This work centers around planning ABE schemes with quick decryption algorithms. They confine their regard for expressive frameworks without system-wide limits, for example, putting a cutoff on the number of attributes utilized in a cipher-text or a private key. In this setting, they presented the first KP-ABE framework where cipher texts can be decoded with a consistent number of pairings.

In different distributed frameworks [12], a remote client should possibly have the capacity to get to information only when he owns an obvious arrangement of certifications or qualities. By and by, the main strategy for forcing such methodologies is to utilize a trusted server to preserve the information and arbitrate access control. Nevertheless, the secrecy of the information will be undermined just when any server putting away the information is undermined. In this paper, they clarified a framework for registering compound access control on encrypted information which is called as Cipher-text-Policy Attribute-Based Encryption. By the assistance of these strategies, the encrypted data can be stayed quiet regardless of whether the capacity server is suspicious. Furthermore, these techniques are secret against arrangement assaults/attacks. Attributes were utilized to depict the encrypted information and develop strategies into client's keys, in the old Attribute Based Encryption frameworks; while in their framework, attributes takes the necessary steps of portraying a client's certifications; and a gathering encrypting the information will decide a system for who can decode. Hence, their techniques are thoughtfully nearer to ordinary access control strategies, for example, Role-Based Access Control (RBAC).

III. PROBLEM STATEMENT:

Various incalculable ABE plans were proposed. A significant number of these plans expect that the cloud storage service providers taking care of key management are believed and they can't be hacked; nevertheless, practically speaking there might be a few organizations that may stop correspondences among clients and cloud storage providers and after then forces storage providers to discharge client secrets by utilizing government control or different methods. In such cases, encrypted information must be known and storage providers will tend to discharge client secrets. There are two types of ABE, CP-ABE and KP-ABE that were proposed by Sahai and Waters. They raised a suggestive method to relate any monotonic equation as the arrangement for client secret keys. Bethencourt et al. proposed the first CP-ABE. This plan utilized a tree access structure to express any monotonic formula over attributes as the arrangement in the cipher-text.

IV. METHODOLOGY:

The system architecture gives a brief description about the encryption process and decryption process of how the end user and the data owner are involved.

The following are the phases/modules involved in the process:

1. Data owner
2. Cloud server
3. Key Distribution Centre
4. Data consumer/End user
5. Attacker/Unauthorized user

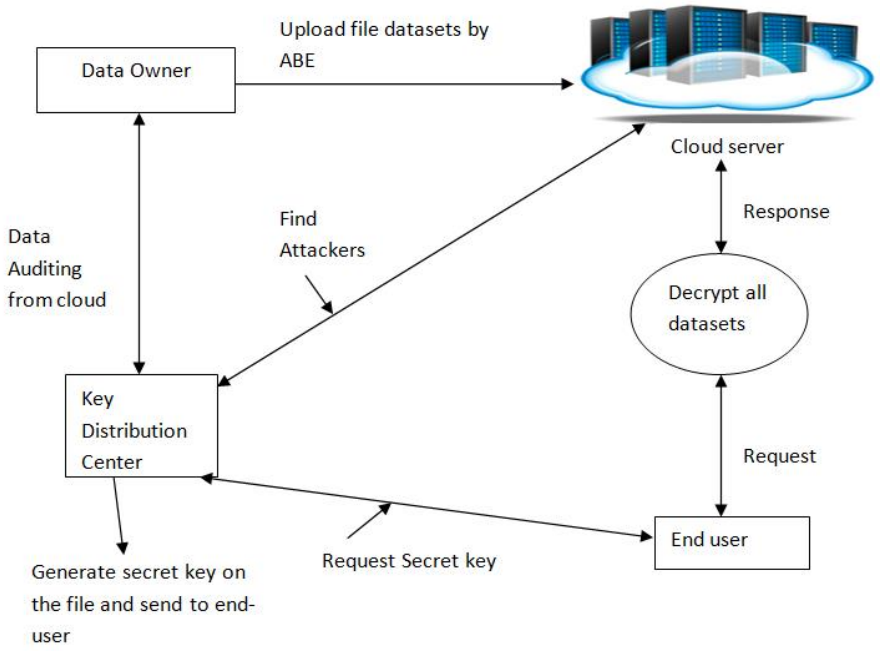

Figure 1: System Architecture

Data Owner:

The data owner must know about the business impact of a security occasion that outcomes in loss of accessibility, privacy or integrity. Even though the cloud services provide various advantages, a venture must answer the most crucial inquiry while going for any cloud facilitated administration that is "who is the owner of data". In this module, the data owner moves the information into cloud server. Because of the security, data owner encrypts information record and after that stores it in the cloud. The Data proprietor can set the access favorable position to encrypted data file.

Cloud Server:

A cloud server is normally known as virtual server that keeps running in a cloud computing condition. It is assembled and provided by means of a distributed computing platform which is the Internet, and can be accessed remotely. The Data proprietors encode the information documents and after that store it in the cloud so as to impart it to customers. To get to these documents, the buyers download encrypted information records from the cloud and after that decrypt them.

Key Distribution Center:

A key distribution center (KDC) in cryptography is answerable for providing keys to the users in a network which shares delicate or personal data. This key distribution center is a form of symmetric encryption which allows the access of two or more systems in a network thereby creating a distinctive ticket type key for initiating a certain connection over which data is shared and shifted. It is responsible for capturing the attackers. Instead of standard key encryption, KDC can be used and the chances of attack will be minimized as the key is generated every time a connection is requested.

Data Consumer/End User:

The “end” part of the term possibly obtained from the fact that most information technologies involve a series of interconnected outcome elements at the end of which is the “client/user”. In this module, the client can possibly get to the information file with the encrypted key if the client has the benefit to approach the document. For the client level, various benefits of interest are given by the Data proprietor and the Data users are controlled by the data owner only.

Attacker /Unauthorized User:

The cloud computing models have full of privileges when compared to on-the-spot models, they’re still susceptible to both inside and outside attacks. Hence, cloud developers need to take security plans to protect their users’ delicate data from cyber attacks. Attacker attaches the malicious data to a piece in cloud server.

4.1 SCHEME DESCRIPTION:

As the greater part of the deniable encryption is bitwise they are incompetent to the genuine use particularly in the cloud storage service case. To take care of this issue, the utilization of hybrid encryption scheme that utilizes symmetric and asymmetric encryption they utilize a deniably encrypted arrangement ahead symmetric information encryption key, while genuine information are encoded by a symmetric key encryption mechanism for the most part deniable encryption plans have decryption error issues was taken into consideration. These errors

originate from the thought about decrypting mechanisms that utilizes the subset decision mechanism for decryption, the receiver chooses the decrypted message as per the subset decision outcome. If the sender wants a component from the universal set, however unfortunately the component is situated in the particular subset, at that point a mistake happens.

The indistinguishable mistake happens in all transparent set- based deniable encryption occurs. The scope of procedure of a record may be unused by the client's request, at the time of termination of an agreement or the documents are moved totally for one cloud to the following cloud's space. The position when any of the above criteria exists the approach will dismiss and the key chief will absolutely pull back from the open key of the related document. So nobody can get the control key of a repudiated document in future. Because of this reason we can say the document is absolutely deleted.

To get well the document, the client must request the key controller to manufacture the public key and the client must be confirmed. The KP-ABE standard is used for record get to which is affirmed by methods for an attribute associated with the document.

A. Deniable Encryption Process:

This procedure incorporates senders and receivers making verification of fake information in cipher texts with the end goal that outside coercers are pleased and hence the coercers can't locate the revealed information if it is valid or not. This scheme attempts to put the endeavors of coercers in vein. The utilization of this procedure is done with the end goal that cloud storage providers can give scrutiny-free storage services. The information proprietors/data owners are called as senders and the people who alter the information are called as receivers. The information scheme, including the cloud storage providers themselves, who has all the secrets must probably decode all encoded information. The ABE attributes for encrypting stored information with an ideal access control system and deniable encryption to anticipate outside investigation is used.

B. Composite order Bilinear Group:

Firstly, structure a deniable CP-ABE scheme with Composite order bilinear groups for making scrutiny-free cloud storage services. Composite order bilinear gatherings (groups) contain two properties: projecting and cancelling. Cancelling property is utilized for predictable condition; then again, Freeman additionally called attention to the critical issue of computational expense with respect to the Composite order bilinear gathering. The Composite order bilinear gatherings activities are slower than prime order bilinear gatherings tasks. In this plan, a client will invest an excessive amount of energy in decrypting while at the same time getting to documents from the cloud. To make Composite order bilinear gathering plans progressively unique, into prime request plans, both projecting and cancelling can't be parallel accomplished in prime order gatherings. For a similar reason, the usage of a recreating tool is projected to change over Composite order bilinear gathering plan to a prime order bilinear gathering plan. This device depends on double unusual bases and the subspace assumption. Dissimilar to subgroups are simulated as various orthogonalized and standardized bases and in this manner, by the symmetrical property, the bilinear activity will be dropped between various subgroups. CP-ABE utilizes cancelling property for Composite order groups.

C. Attribute-Based Encryption:

The services of cloud storage like higher accessibility and security made cloud storage progressively famous. The users can store their data and can also access it from anywhere at any time. The main reason is that the client’s data should be protected. Thinking about the collaborative property of the cloud, attribute based encryption (ABE) is viewed as a standout amongst the most reasonable and effective encryption plans for cloud storage. There are numerous ABE plans that have been presented and most of them describes that the data cannot be revealed but in the present situation some cloud providers loss communication with users and tend to reveal users data to the coercers. If this occurs, then the coercers monitor the confidential data of the user.

4.2 ALGORITHMS USED:

- Dec(PUP,SEK,CT) -> {M} : This decryption algorithm takes the input as public parameter PUP, Private key SEK and the ciphertext CT and returns output as M.
- KeyGen(MSK,S)→SEK : This algorithm takes set of attributes S and MSK(System Master Key) as input and generates output as private key SEK.
- Enc(PUP,M,A) →C :This encryption algorithm takes input as public parameter PUP, message M and LSSS(Linear Secret Sharing Scheme) access structure A .This algorithm encrypts M and outputs a cipher text C.

V. EXPERIMENT ANALYSIS:

In this segment, the performance is estimated by two deniable schemes: Prime order scheme and Composite order scheme. These two schemes are compared with the waters scheme. The performance of the encryption and decryption is estimated by the following fig1 and fig2 by taking number of attributes and the time taken in millisec (msec) along x-axis and y-axis. The no. of attributes are fixed by the user when he encrypts the file and if the user wants to decrypt the file he must be able to match the no. of attributes that were set by the user along with the cipher text . As the number of attributes increases the time taken to encrypt a file or decrypt a file increases. From the above figures, the time along y-axis starts from 0 to 2500 and the no. of attributes starts from 0 to 8. In the Prime order scheme as the no. of attributes increases from 0 to 10 the time taken to encrypt or decrypt a file increases slowly till 500 which is almost equal to that of waters scheme. Whereas, in the Composite order scheme as the no. of attributes increases from 0 to 8 the time taken to encrypt or decrypt a file increases quickly till 2500. Therefore, the performance to encrypt or decrypt a file is better in prime order than in Composite order scheme.

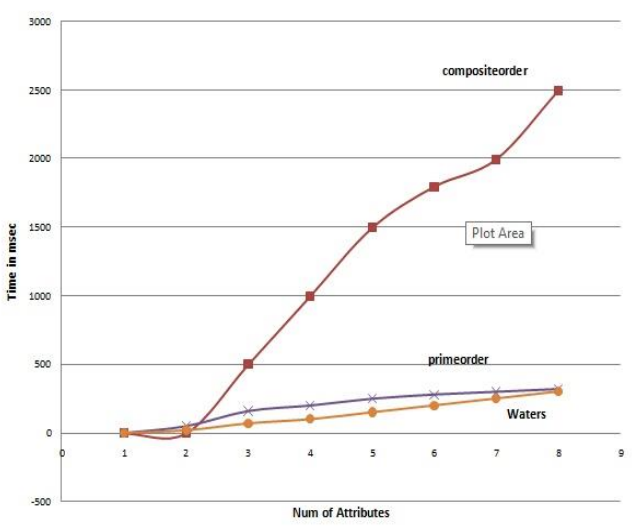

Figure 2: Encryption

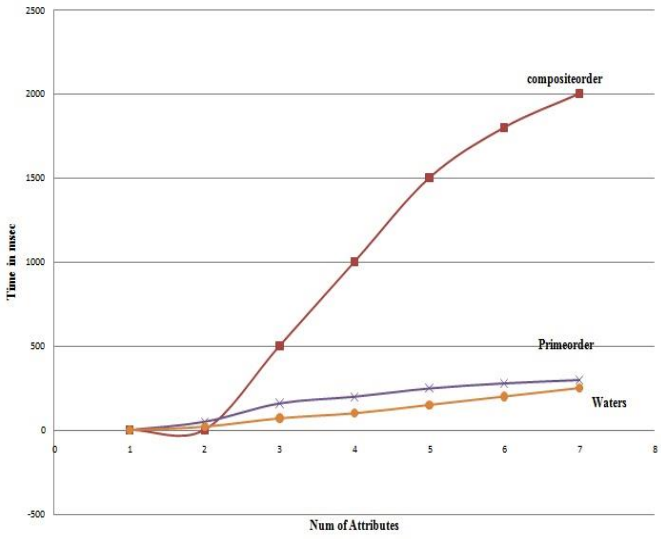

Figure 3: Decryption

VI.CONCLUSION:

In this work, we deployed a scheme of CP-ABE which is able to another sort of encrypted access control. This plan expresses client's private keys by a lot of attributes and party encrypting information can express an approach over these attributes by specifying which users are able to decrypt. Our scheme allows policies to be conveyed as any monotonic tree access structure and is unaffected to collusion attacks in which an attacker may acquire multiple private keys. In future, it would be absorbing to consider ABE schemes with different types of expressibility. Whereas, KP-ABE and CP-ABE are two schemes that were clearly existed in other schemes. The basic challenge in this work is to provide a new scheme with refined forms of expression that generate more than an arbitrary combination of techniques. We trust an important attempt which would be to prove a system secure under a more grade and non-interactive assumption. This type of work would be more engaging if it results in a modest loss of efficiency from our existing system.

REFERENCES:

[1]N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ra`fols, "Attribute-based encryption schemes with constant-size cipher texts," Theor Comput. Sci., vol. 422, pp. 15–38, 2012.

[2] D. M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in Eurocrypt, 2010, pp. 44–61.

[3] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Israel Institute of technology, 1996.

[4]M. H. Ibrahim, "A method for obtaining deniable public-key encryption," I. J. Network Security, 2009, vol.8,no.1,pp.1-9.

[5]R. Bendlin, J. B. Nielsen, P. S. Nordholt, and C. Orlandi, "Lower and upper bounds for deniable public-key encryption," Cryptology ePrint Archive, Report 2011/046, 2011,http://eprint.iacr. org/.

[6]M. Du¨rmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in Eurocrypt, 2011, pp. 610–626.

[7]Tanuj Sharma, Lakhan Singh Asst.Prof., Ankur Taneja Asst.Prof., International Journal of Scientific Research & Sept-Oct- 2018, Engineering Trends Volume 4, Issue 5.

[8]M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical deniable encryption," in SOFSEM, 2008, pp. 599–609.

[9]Dr. Jammi Ashok Professor, Dr. G. Nanda Kishor Kumar Associate Professor, International Journal of Innovations & Advancement in Computer Science IJIACS November 2017, ISSN 2347 – 8616 Volume 6, Issue 11.

[10] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in WPES, 2010, pp. 31– 42.

[11]S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.

[12] John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption", in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[13] Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[14]. Jegadeesan,R.,Sankar Ram, R.Janakiraman *September-October* 2013 "A Recent Approach to Organise Structured Data in Mobile Environment" R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[15]. Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar [1], Supervisor[2], VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[16]. Jegadeesan,R., Sankar Ram, M.S.Tharani *(September-October, 2013)* "Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology *G.J. E.D.T., Vol. 2(5): Page No:9-14* ISSN: 2319 – 7293

[17]. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., *January 2014* "NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD" *Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793* Vol: I Issue XIII, Page No: Impact Factor:0.433

[18]. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 "SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[19]. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology

[20].Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[21]. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[22]. Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[23]. Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[24]. Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[25]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

[26]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.