Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

# Enhanced Public Key Encryption with Keyword Search in Cloud

M. Sowmya Lakshmi
M. Tech, Department of CSE, JNTUACE
Anantapur, India

S. Vasundra
Professor, Department of CSE, JNTUACE
Anantapur, India

***Abstract*-The Industrial Internet of Things is flourishing, which is incredibly directed by the snappy improvement of remote sensor structures with the help of dispersed enlisting. There are already self-driving cars and e-health facilities that monitor people's wellness. There is a tremendous opportunity for IOT and industrial internet to pull digital devices to assist in personal lives. Cloud Computing is intended and supported primarily as a data center and an effective communication with the outside world. Lightweight Searchable Public-Key Encryption (LSPE) has given semantic security under the computational bilinear diffieHellman supposition in the irregular prophet.. The main aim of proposed framework is improving the LSPE model as far as expense and essentialness for creating the ciphertext. In the proposed structure, where the data sender scrambles a watchword as well as validates it to persuade a verifier that the encoded catchphrase must be create by the sender.**

***Index Terms:- Cloud Computing, Industrial internet of things ,Lightweight Searchable Public-Key Encryption (LSPE), Key aggregate encryption(KAE), Smantic security.***

## I. INTRODUCTION

Late improvements in IT have made it a lot simpler to store and share data remotely. New applications, for example, online interpersonal organizations and online archives give helpful approaches to individuals to store and share different information including individual profile, electronic reports on remote online information servers. Distributed computing, viewed as the future IT engineering, even guarantees to give boundless and flexible capacity asset (and other figuring assets) as a support of cloud clients in a very savvy way. Albeit still at its beginning period, Cloud Computing has officially drawn incredible consideration, and its advantages have pulled in an expanding number of clients to re-appropriate their nearby server farms to remote cloud servers. On one hand, revelation of delicate data, for example, wellbeing records, put away on remote information servers must be carefully secured before clients have freedom to utilize the information administrations. Fine-grained information access control components frequently should be set up to guarantee suitable exposure of delicate information among different clients. Then again, in remote information stockpiling clients don't physically have their information. Remote information specialist organizations are practically sure to be outside the clients' trust space, and are not permitted to get familiar with clients' touchy data put away on their servers. Things being what they are, clients can't depend on remote information servers to implement access control arrangements like customary access control in which reference screens ought to be completely trusted. Client implemented information access control is in this way profoundly wanted for remote information stockpiling. This composition watches out for the issue of confirming data sharing on untrusted amassing by examining cryptographic procedures to empower customers to execute data get to approaches just encoded data are secured on limit servers while holding riddle key(s) to the data owner herself; customer access is yielded by issuing the relating data unravelling keys.

In particular, we think about novel open key cryptography – Attribute-Based Encryption (ABE), and improve it toward giving an unquestionable cryptographic explanation behind a protected data sharing arrangement on untrusted amassing. In view of ABE, we likewise present our answers for verifying information partaking in Cloud Computing and remote sensor arranges individually.

In untrusted stockpiling information servers are not permitted to become familiar with the substance of delicate information, nor would they be able to be depended on to implement information get to strategies. To keep information secret to information servers the information proprietor encodes information before transfer. Client access is conceded by having the information decoding key(s).When this kind of cryptographic based access control plan give security protection on data, there are similarly a couple of essential challenges identified with the arrangement structure. We can abridge the difficulties as pursues, for example, ACL-based access control [3], capacity based access control [4], and job based access control [5]. For untrusted stockpiling, one may consider implementing a similar access arrangements like ACL with cryptographic techniques. ACL-based and capacity based access control, when upheld with cryptographic techniques, has the versatility issue. Conventional ACL-based access control requests each datum article to record the rundown of approved clients.. In job based access control [5], get to is conceded by the client's role(s) and the information articles don't have to keep the approved client list. Authorizing these entrance approaches with cryptographic techniques needs to address different assaults, for example, client agreement, in which clients with various jobs (i.e., the relating decoding keys) endeavor to acquire additional entrance benefits by sorting out their keys (i.e., jobs).

There are a few late work [3] in the territories of "shared cryptographic record frameworks" and "access control of re-appropriated information" tending to the comparative issue of information access control with

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

traditional symmetric-key cryptography or open key cryptography. At the point when these plans are reasonable for ordinary document frameworks, the majority of them are less appropriate for fine-grained information access control in huge scale server farms which may have an enormous number clients and information records.

## II. RELATED WORK

Attribute based encryption (ABE) offers the capacity to scramble information without accurate learning of the collector set. In this sense the idea of ABE is firmly identified with RoleBased/Attribute-Based Access Control and reasonable for huge scale applications.

Existing developments of ABE center around giving the fundamental functionalities, for example, information encryption/unscrambling and plot opposition. Before ABE can be connected in functional frameworks there are as yet a few test security issues to be tended to as portrayed in following segments. A viable and effective client the board component ought to be set up to arrangement with client access benefit award and renouncement. Specifically, client key (and subsequently access benefit) denial is dependably a test issue in cryptography. Existing arrangements propose partner termination time ascribes to client mystery keys. These sorts of assaults are amazingly unsafe for copyright-touchy applications since it extremely simple for key abusers to copy and disseminate information decoding keys to others by ways, for example, email. As the expense of doing this is incredibly low, it is more dangerous than straightforwardly conveying the information itself. Complete counteractive action this sort of assaults is generally accepted to be hard. Regular practice against these assaults is to give a path to the information proprietor to follow any suspicious privateer gadget and gather confirmations of key maltreatment by revealing the illicit key wholesaler's character. At that point the information proprietor can sue the unlawful key wholesalers by introducing these confirmations to law specialists. In doing as such, it necessitates that the client unscrambling key is by one way or another associated to her character.

In ABE, a client mystery key is characterized over qualities and does not have the balanced correspondence with a specific client.To guard against key maltreatment assaults, we can play a similar trap in ABE as double crosser following at an abnormal state see. Be that as it may, hidden procedures embraced by existing double crosser following frameworks can't be legitimately connected to ABE on the grounds that collectors are spoken to independently in traditional communicate encryption while not in ABE. Specifically, the information proprietor might want to keep her entrance strategy data private to servers and clients may have worries on unveiling their entrance benefit data to servers. In existing developments of ABE, either the entrance arrangement or characteristics ought to be connected in plaintext to the information ciphertext to encourage client decoding.

For protection conservation, it is important to give another development to ABE to conceal the entrance approach or qualities. Beside the above general test issues, there are likewise numerous other application explicit difficulties. Proficiency is one of them and various applications would have various prerequisites on it. Current development of ABE presents costly activities, for example, bilinear pairings on scramble and additionally decode, which are not really reasonable to the gatherings. It is alluring either to search for effective developments for ABE, or to join ABE with different calculation appointment strategies to offload the calculation escalated activities to all the more dominant gadgets.

## III. PROPOSED WORK

In Key Aggregate Cryptosystem, customers encode their information under an accessible door, yet what's more underneath an identifier of figure substance called class and those figure plays are additionally isolated into specific classes. The information proprietor holds a key called Master mystery key. The ace mystery can be used to create mystery keys for particular classes. All the more fundamentally, the produced key can be a total key which is as strong as a mystery key for a solitary class, yet consolidates the expert of numerous such keys, with the end goal that the decoding level for any subset of figure content classes.

By these goals, Alice can neatly send Bob a special total key through a safe channel like email. Bob can download the scrambled information from the Drop box space of Alice and then use this overall key to decode this encoded data. Figure 2.1 shows the circumstances. As the image traces, Alice will shop her very own photos on the drop rack and she accept that nobody can get to her photos.. Because of information misfortune prospect Alice does not have a sense of safety and she scrambles the whole pictures utilizing her own key before transferring.

### *A. KAC Data Sharing Structure*

Now Alice wants to share some of her pictures with Bob. Now here comes to issues for data sharing. Alice has to follow the below two procedures to share her data.

1. Alice has to encrypt all the pictures with one encryption key and share that secret key with bob.
2. Encrypt each picture with a special key and send corresponding secret keys to bob for individual pictures.

The first way is not secure because all the pictures are leaked to bob.

The second procedure results in loss of efficiency because number of cipher text classes is increased with the increase of number of keys. There will be various keys as many as numbers of pictures are encrypted.

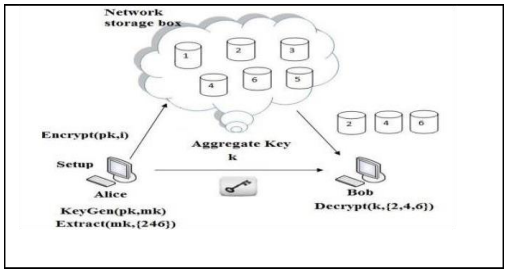


Fig: KAC data sharing structure

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

Sharing of these keys needs a secured channel and securing these keys need a sheltered storing. The cost and issues incorporate all things considered augmentations with number of unscrambling keys to be share.

To maintain a strategic distance from these to issues the Key Aggregation is utilized, where a solitary total key is produced for chosen number of pictures and Alice sends that total key to Bob which prompts a better and effective method for key stockpiling and decreases the quantity of figure content classes and furthermore the correspondence cost to move the keys and the capacity cost to store a solitary key as opposed to numerous keys.

THE PROCEDURE OF KEY AGGREGATION IS AS FOLLOWS:

*Setup Phase*
The Alice (data owner) runs the setup phase for an account creation on server in an untrusted way. The setup scheme only considers implicit security parameters.

*Key Gen Phase*
This phase is run by Alice to generate the master key or the public key pair (pk, msk).

*Encrypt Phase*
Encode (pk, m, I), the encryption scheme sees input as accessible parameters pk, letter m, and I, indicating category ciphertext. The plan encodes message m and produces a ciphertext C with the end goal that solitary a solitary client who has the arrangement of characteristics that guarantee the entrance structure will most likely decode the message.

- Input = message m, public key pk, and an index i.
- Output = ciphertext C.

*Extract Phase*
This phase is run by the Alice for hand over the decrypting authority for a definite set of ciphertext classes to a delegate.

- Input = master main mk and a range of indicators matching distinct categories Figure: KAC Data sharing structure
- Outputs = kS marked aggregate key for fixed S.

*Decrypt Phase*
The person (Bob) who has the authority to decrypt is operating this stage. Decrypt (kS, S, I C), the decryption phase defines input as pk, ciphertext C, ciphertext categories for a collection of characteristics
S.

- Input = kS and segment S, where item I = category of ciphertext
- Outputs = m if item S is used.

*B. Leakage Resilience*
This venture utilizes the hash proof algorithm that builds a leakage-resilient IBE (LR-IBE) .In proposed framework this undertaking uses personality based encryption in this calculation for every character id, there are different substantial mystery keys slide and furthermore two various types of ciphertexts: valid and invalid. The thought is to include an extra measure of haphazardness to our character based mystery keys, called the label t, appended with some ace key terms. This is done in a mode that the mystery key holder can now basically re-randomize the key along the exceptional level of opportunity which is required for the first verification, but can no longer re-randomize the key along the new tag-measurement to any further degree. This will give us a chance to portray invalid ciphertext which decode to unsystematic qualities when the label t is arbitrary, but unscramble to the indistinguishable worth when the label t is kept indistinguishable, however the key is re-randomized along the first level of opportunity.

ADVANTAGES OF LEAKAGE RESILIENT SYSTEM ARE

- To secure against frail key-spillage assaults
- Efficient and adaptable for key assignment.
- The number of ciphertext classes save progressively.

The Leakage Verification Process is depicted below:

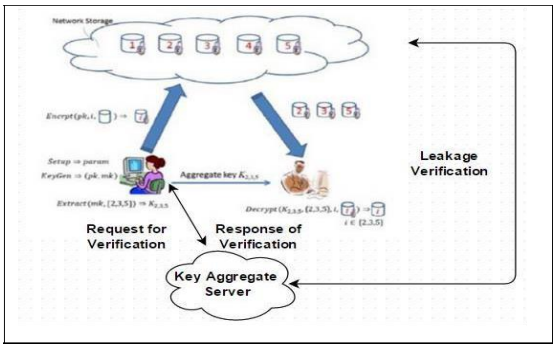


Figure: Leakage Verification Structure.

As the above figure depicts that the Alice maintains a Key Aggregate Server (KAS) which is responsible for key generations and data storage. As the data is uploaded the KAS generates an individual signature on each file and stores that in two places:

- Cloud Server
- KAS

Whenever Alice wants to verify whether there is a leakage occurred or not she sends a request to KAS along with the file name and that KAS fetches the signature from the Cloud server for that specific document and contrasts and the put away signature in the event that the marks are changed, at that point sends an affirmation to Alice that the information has been spilled else demonstrates that information is dangerous.

## IV. RESULTS

The proposed KAC system along with the leakage resilience is tested undertow metrics

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

- Key generation time
- Delegation Ratio

The first metric defines how fast the proposed scheme generates signature and keys for a given set of data in graph.

As the graph clearly depicts that the ABE needs more time as the size of the data increases but the proposed scheme consumes constant time irrespective of the data size.

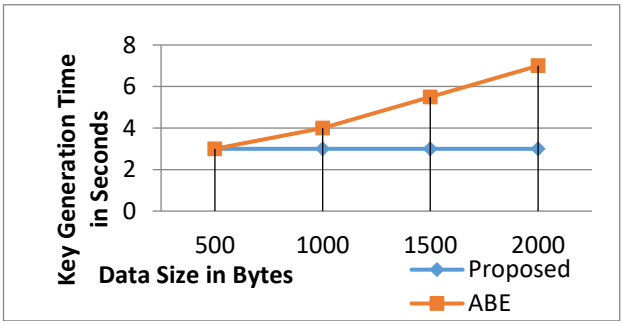


Figure: Key generation time

The next metric is the delegation ration**.** Then again, to decode ciphertext for a lot of classes, once in a while the agent may need to hold countless keys, as delineated in below graph.

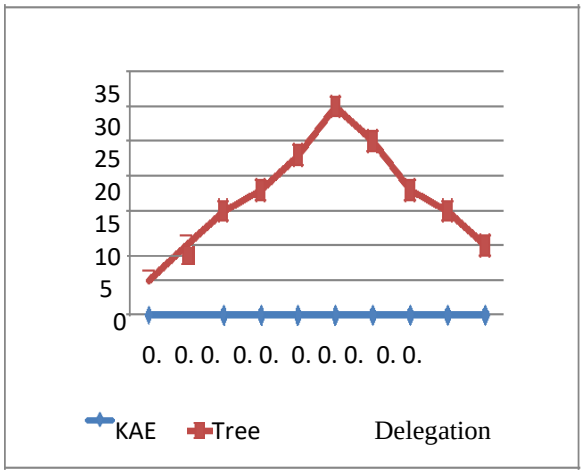


Figure: No. of key generation

In this way, we are keen on na, the quantity of symmetric keys to be doled out in this various leveled key methodology, in a average sense. We assume that there are actually 2h ciphertext classes, and the delegate of concern is qualified for a part r of them. In other words, r is the ratio of the delegation, the ratio of the designated classes of ciphertext to the overall classes. Clearly, if r = 0, na ought to likewise be 0, which means no entrance to any of the classes; if r =100%, na ought to be as low as 1, which implies that the ownership of just the root key in the chain of importance can allow the entrance to all the 2h classes. Therefore, one may expect that na may initially increment with r, and may diminish later. We set r = 10%; 20%; . . . ; 90%, and pick the segment in an irregular way to display a discretionary "designation design" for various representatives.

The performance is compared between KAE (key aggregate Encryption) and tree based key task in [1] and the outcomes are delineated beneath.

The results depicted clearly shows that the proposed has a constant delegation ration.

## V. CONCLUSION

To share data among the users efficiently is crucial thing in cloud computing. Users favor to upload there data on cloud and among different locations. Outsourcing information to the server may result in the exposure of user's private data to unauthorized people. Encryption is a promising arrangement which offers to impart chosen information to favored hopeful. Sharing of decryption keys in secure way plays significant role. Public key cryptosystems assign secret codes in distributed storage to different cipher text categories. The representative securely gets a set size aggregate key. It is necessary to keep sufficient number of cipher texts classes as they increase fast with respect to the keys. This project provides a Key Aggregate Cryptosystem along with the leakage resilience to data. The performance is promising and the verification of leaked data is efficiently handled by the key aggregate server.

## REFERENCES

[1] Cheng-Kang Chu, Sherman S.M. Chow, **"**Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage**"** IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 2, FEBRUARY 2014, pp. 468-477.

[2] D. Zeinalipour-Yazti, V. Kalogeraki, D. Gunopulos, A. Mitra, A. Banerjee, and W. Najjar, "Towards in-situ data storage in sensor databases," in PCI'05, LNCS 3746, Volos, Greece, 2005, pp. 36–46.

[3] ACL. http://en.wikipedia.org/wiki/Access control list

[4] H. M. Levy, "Capability-Based Computer Systems", Digital Equipment Corporation 1984. ISBN 0-932376-22-3.

[5] NIST. "Role Based Access Control (RBAC) and Role Based Security". http://csrc.nist.gov/groups/SNS/rbac/

[6] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Over-encryption: Management of Access Control Evolution on Outsourced Data. In Proc. of VLDB'07, Vienna, Austria, 2007.

[7] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus: Scalable Secure File Sharing on Untrusted Storage. In Proc. of FAST'03, Berkeley, California, USA, 2003.

[8] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003.

[9] Dr. S. Vasundra *et.al*, CSE, JNTUACEA, Published a paper" Enabling Secure Data Sharing in the Cloud Storage Groups", International Research Journal of Engineering and Technology, ISSN: 2395-0056, July 2017.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy reencryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005

[11] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2007.

[12] Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.

[13] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.

[14] R. Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non- monotonic access structures". In Proc. of CCS'06, New York, NY, 2007

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 08, August-2019

**M. Sowmya lakshmi** received B.Tech degree from intell engineering college anantapur in 2010. Currently pursuing M.Tech in software engineering from JNTUA College of Engineering
Anatapuram.

**Dr. S. Vasundra**, Professor, Department of CSE, JNTUA College of engineering autonomous, Ananthapuramu, and she has 20 years of teaching experience and completed PhD in the year of 2013. Research interests are Mobile Ad hoc Networks, Computer Networks, and Big Data, data warehousing and data mining, cloud computing. Published more than 60 international journals and attended 30 international conferences and also worked various academic roles in JNTUA University. Presently working as NSS coordinator in JNTUA University.