IJRSET NOVEMBER 2018 Volume 5, Issue 11 Pages: 15-22

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

DATA SECURE IN MOBILE COMPUTING USING ATTRIBUTE BASED ENCRYPTION DSA - CP-ABE

[1] A. Nandhini, [2] Mrs. S. Anuradha, M.Sc, MCA, M.phil, (SET)
[1] M.Phil Scholar CS, [2] Assistant Professor of CS
[1, 2] Shri Sakthikalaish Woman's College
[1, 2] Salem.

ABSTRACT- Cloud has been around for two decades and it consists of the vast amount of data from all over the world. Most of the people at a personal level and organization level have moved their data to the cloud and share data across all around the world. The ubiquity of distributed computing, cell phones can stock and recover sensitive data from cloud whenever. Therefore, the information security issue in versatile cloud tries out to be increasingly extreme and forestalls advance improvement of portable cloud. There are generous examinations that have been run to enhance the cloud security. Be that as it can, a big slice of them are not relevant for versatile cloud since cell phones just have constrained registering assets and power. Arrangements with low computational upstairs are in awesome requirement for versatile cloud applications. In this paper, we proposed a (DSA) for portable distributed computing. It embraces CP-ABE, an entrance control innovation utilized as a part of typical cloud condition, yet changes the construction of access regulator tree to make it reasonable for portable cloud conditions. DSA moves an extensive section of the computational genuine access control tree change in CPABE from mobiles to outside go-between servers. Moreover, to decrease the client repudiation cost, it acquaints quality portrayal fields with execute lethargic disavowal, which is a prickly issue in program based CP-ABE substructure. The exploratory outcomes demonstrate that DSA can successfully lessen the overhead on the cell phone side when clients are sharing information in portable cloud conditions.

Keywords: [Communication, Measurement, Storage, Attribute Based Encryption]

1. INTRODUCTION

Cloud computing means storing data and accessing that data from the Internet instead of Using Traditional hardware for most of the operations. More than 50% of IT companies have moved their Business to the cloud. Sharing of data over the cloud is the new trend that is being set on. The amount of data generated on a day to day life is increasing and to store that all of the data in traditional hardware is not possible because of limited storage capacity. Therefore, transferring the data to the cloud is a necessity where the user can get unlimited storage. Security of that data over is the next big concern for most of us. After uploading the data to the cloud use loses its control over that data. Since personal data files are

sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Therefore, privacy of the personal sensitive data is a big concern for many data owners. When any of the people upload the data onto the cloud they are leaving their data in a place where monitoring over that data is out of their control, the cloud service provider can also spy on the personal data of the users. When someone has to share data over the data they have to share the password to each and every user for accessing the encrypted data which is cumbersome. Therefore, to solve this problem data should be encrypted before uploading it onto the cloud which can be safe from everyone. Now the data encryption part brings some new problems such as we have to provide an efficient encryption algorithm such that if the data Is in encrypted format it cannot be easily to get break or get accessed by any exploiters.

The advancement of distributed computing and the ubiquity of shrewd cell phones, individuals are bit by bit getting acclimated with another period of information sharing model in which the information is put away on the cloud what's more, the handsets are utilized to store/recover the data from the cloud. Commonly, cell phones just have constrained storage room and figuring power. On the contrary, the cloud has massive amount of resources. In such a condition, to accomplish the tasteful execution, it is fundamental to utilize the assets gave in the cloud dedicated co-op (CSP) to stock and offer the information. These days, different cloud versatile claims have been generally utilized. In these applications, individuals (information proprietors) can transfer their photographs, recordings, reports and different documents of the cloud and offer these data with different people (data customers) they get a boost out of the opportunity to share. CSPs additionally give information administration usefulness to data managers allowed. Since individual information documents are touchy, information proprietors are permitted to pick whether to make their information records open or must be imparted to particular information clients. Plainly, information protection of the individual touchy information is a major worry for some information proprietors. The best in class benefit administration/get to control components gave by the CSP are either not adequate or not extremely helpful. They can't seen all the prerequisites of data managers. To begin with, when individuals transfer their data records onto the cloud, they are leaving the information in a place where is out of their control, and the CSP is used to watch the client data for its business advantages as the different reasons. Second, individuals need to send secret key to every datum client on the off fortuitous that they just need to pass the encoded information with specific clients, which is extremely awkward. To rearrange the benefit administration, the data manager can partition information clients into various gatherings and send secret key to the gatherings which they need to pass the information. Notwithstanding, this approach requires fine-grained get to control. In the two cases, secret key administration is a main issue. Plainly, to handle the above points, individual sensitive data ought to be encoded before exchanged onto the cloud with the objective that the data is secure with the CSP. In any situation, the data encryption brings new issues. Well-ordered guidelines to give profitable access control segment on ciphertext unscrambling with the objective that solitary the endorsed customers can get to the plaintext information is testing. Also, framework must offer information proprietors compelling client benefit administration ability, so they can give/renounce information get to benefits effortlessly on the information clients. There have been

significant explores on the issue of information get to control over ciphertext.

2. LITERATURE SURVEY

R.Gokula Priya , Unnimaya P Madhu, M.Yuvashree, M.Karthikeyan(2018) proposed a lightweight data sharing scheme (DSA) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that DSA can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments. Achyuth Ranjan V , K. Karthikayani , P. Jaswanth , Vivekananthan GR , Shankara Lingam(2018) proposed It embraces CP-ABE, an entrance control innovation utilized as a part of typical cloud condition, yet changes the construction of access regulator tree to make it reasonable for portable cloud conditions. DSA moves an extensive section of the computational genuine access control tree change in CPABE from mobiles to outside go-between servers. Moreover, to decrease the client repudiation cost, it acquaints quality portrayal fields with execute lethargic disavowal, which is a prickly issue in program based CP-ABE substructure. The exploratory outcomes demonstrate that DSA can successfully lessen the overhead on the cell phone side when clients are sharing information in portable cloud conditions. Chandni Patel , SameerSingh Chauhan , Bhavesh Patel (2015) proposed framework the cryptographic methods as well as algorithms are used for encryption and decryption of mobile user data. This Framework ensures the additional security and confidentiality of user‟s sensitive or significant data. This paper introduces the scheming flow of proposed security framework. This proposed Security framework is for the purpose to secure and provide privacy and integrity to user‟s confidential data in Mobile Cloud Environment. Puja Pingale , Dipanjali Gaikwad , Ashwini Bhapkar , Rutuja Pharande , Monika Waghmare (2017) proposed Mobile device has limited storage and limited computing resources so data can be stored on mobile cloud computing .Any user can upload data on that cloud also anyone can access that data, so there is security issue related to that data so, we need to provide security to that data to prevent from unauthorized user. Now a days, the cloud computing becomes more popular but the security is not provided in efficient manner. The issues related to security is increases day by day. Some algorithms are designed to provide security to cloud computing but those are not efficient for mobile cloud computing so we design DSA -CP-ABE algorithm for provide security to the mobile cloud computing. DSA migrates major computational overhead from mobile client side devices using proxy servers. Also we can use lazy re-encryption method which can reduce time consuming process. Lightweight secure data sharing scheme can reduce the computational overhead on the client side mobile device when users are sharing their data on mobile cloud . Also we use the AES (Advance Standard Encryption) algorithm for data encryption and decryption purpose. Princy P. James , Renuka Ajay Sonone , Naveen Ghorpade , Reddy Kumar V (2018) proosed a lightweight data sharing scheme (DSA) for mobile cloud computing. It adopts CP-ABE (Attribute Based Encryption), an access control technology used in normal cloud environment, but changes the structure of access control tree

to make it acceptable for mobile cloud environments. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a delicate issue in program based CPABE systems. The experimental results show that DSA can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

3. PROPOSED WORK

3.1 CP-ABE Algorithm

In this paper, we propose a Data secur attribute (DSA) for mobile cloud computing environment. We design an algorithm called DSA-CP-ABE based on Attribute Based Encryption (ABE) method to offer efficient access control over cipher text. We use proxy servers for encryption and decryption operations. In our approach, computational intensive operations in ABE are conducted on proxy servers, which greatly reduce the computational overhead on client side mobile devices. We are providing methods for efficient access of the data. Performance has been increased with the reduced cost. In ciphertext-framework unmistakable based encryption a client's private-key is associated with an arranging of charecters and a ciphertext chooses a path system over a depicted universe of properties inside the structure.k arranged of n credits must be available (there may in like way be non-monotone access approaches with extra negations and in the interim there are more- over upgrades for strategies depicted as discretionary circuits).For example, let us expect that the universe of credits is depicted to be A,B,C,D and client 1 gets a key to properties A,B and client 2 to property D.On the off irregular that a ciphertext is changed over concerning the strategy (A?C)?D, by then client 2 will be able to mastermind, while client 1 won't have the fitness to interpret. Calculation starting now and into the foreseeable future licenses to see got a handle on guaranteeing, i.e., bolster is joined into the mixed data and essentially people who satisfy the related course of action can arrange data. Another dazzling highlights is, that clients can get their safe keys after information has been mixedSo information can be blended without learning of the honest to goodness procedure of customers that will have the capacity to unscramble, yet simply picking the system which honors to unravel. Any future customers that will be given a key with respect to properties to such a degree, to the point that the approach can be fulfilled will by then can translate the data.

3.2 Secur Data CP-ABE Algorithm

3.2.1 User Authorization

The procedure of client approval executes Function 2 to create property keys for information clients. The particular procedure is depicted as takes after. (1) DU logins onto the framework and sends, an approval demand to TA. The approval ask for incorporates trait keys which DU as of now has. (2) TA acknowledges the approval demand and checks whether DU has signed on previously. In the occasion that the client hasn't signed on previously, go to step (3) , generally go to step (4). (3) TA calls Function 2 to create quality keys (SK) for DU. (4) TA thinks about the trait portrayal field in the quality key with the property depiction field put absent in database. In the occasion that they are not coordinate, go to step (5), generally go to step (6). (5) For each conflicting piece in portrayal field, in the occasion that it is 1 on information client's side and 0 on TA's side, it demonstrates that DU's property has been repudiated, at that point TA does nothing on this bit. In the event that it is switched situation, it demonstrates that DU has been appointed with another characteristic, at that point TA produces the comparing property key for DU. (6) TA checks the adaptation of each quality key of DU. On the off chance that it's not the same with the present adaptation, at that point TA refreshes the

relating quality key for DU. In the phase of client approval, TA refreshes property keys for DU as per the quality depiction field, which is put away with SK. It portrays which traits DU has and their relating variants. TA additionally keeps characteristic portrayal field of DU in database. At the point when DO changes the property of DU, the trait depiction field on the TA side is likewise refreshed. Along these lines, when DU logins on the framework, the property depiction field on itself might be not quite the same as that of TA. TA needs to refresh the trait keys for DU as indicated by the property portrayal field similarly as depicted previously.

3.2.2 Information Confidentiality against Conspiracy

The information privacy is considered from two perspectives. In DSA, information are encoded with a symmetric key. The security of this part is guaranteed by symmetric encryption instrument. Next, the symmetric key is mixed by trademark encryption. The security of this part depends upon the encryption technique. The security of the inside figuring in the encryption method is exhibited in the past region. Here, we talk about the circumstance that the symmetric key is sheltered regardless of whether a malignant client, ESP and DSP planned to get the key. The trick assault can be separated into a few sorts, to be specific intrigue between various clients, DSP and ESP, clients and cloud. To begin with, think about the scheme between various clients. It can be demonstrated that distinctive clients with various properties can't join their credits to decode information records. Since clients get distinctive r from TA, which is utilized to create property keys for clients, diverse clients with same characteristics get diverse keys. While unscrambling information records, just when all the keys are produced from a similar r would they be able to be consolidated to decode information documents, in this way successfully keeping the scheme between clients. Second, think about the intrigue amongst ESP and DSP.ESP gets S1 , Ta and PK from DO and TA, and DSP gets SKu', CT from DU. Joining all these data, ESP and DSP on account of the bilinear diffie-hellman suspicions, hence ensuring CTk. Last, think about the connivance between the cloud and DU. The cloud may send information parcels to whom don't meet the entrance control arrangement. Be that as it may, regardless of whether DU unlawfully gets ciphertext, it can't get the plain setting since it doesn't have the correct characteristic keys.

4. EXPERIMENTAL RESULTS STORAGE OVERHEAD EVALUATION

DES	ABE	Proposed CP-ABE
0.09	0.02	1.3
0.14	0.05	1.8
0.19	0.09	2.1
0.25	0.14	2.4
0.3	0.19	3

Table 1: Comparison table values of Storage Overhead Evaluation

Comparison table 1 explains the values of storage overhead evaluation of existing methods DES and ABE and proposed method CP-ABE. The storage overhead evaluation ratio of DES is 0.3 maximum and minimum is 0.09, the ratio size of ABE is 0.19 maximum and 0.02 minimum and the ratio size of proposed method is 3 maximum and 1.3 minimum. The storage overhead evaluation ratio of DES and ABE is minimum in size than compared to proposed method CP-ABE. Hence that capacity of storage overhead in proposed method is high.

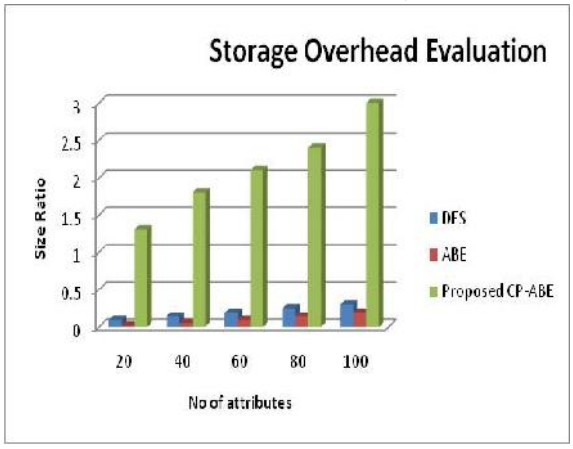

Figure 1: Comparison graph values of Storage Overhead Evaluation

Comparison graph (fig.1) explains the values of storage overhead evaluation of two existing methods DES and ABE and one proposed method CP-ABE. The comparison of two methods is measured using its number of attributes from 20 to 100 and the size of its ratio. The storage overhead evaluation ratio of DES is 0.3 maximum and minimum is 0.09, the ratio size of ABE is 0.19 maximum and 0.02 minimum and the ratio size of proposed method is 3 maximum and 1.3 minimum. It is assumed that the attribute value and the size of ratio in proposed method is high when compared to DES and ABE methods.

Measurement Overhead

DES	ABE	Proposed CP-ABE
0.09	0.02	0.1
0.14	0.05	0.2
0.19	0.09	0.24
0.25	0.14	0.29
0.3	0.19	0.32

Table 2: Comparison table values of Measurement Overhead

Comparison table 2 explains the values of measurement over headed in two existing methods DES and ABE and one proposed method CP-ABE. The ratio of measurement overhead in DES is 0.09 minimum and 0.3 maximum, in ABE the ratio measured is minimum 0.02 and 0.19 maximum and in proposed method CP-ABE the ratio measured is minimum 0.1 and maximum 0.32. It is assumed that the value of measurement over headed in Proposed method is high when compared to two existing methods DES and ABE.

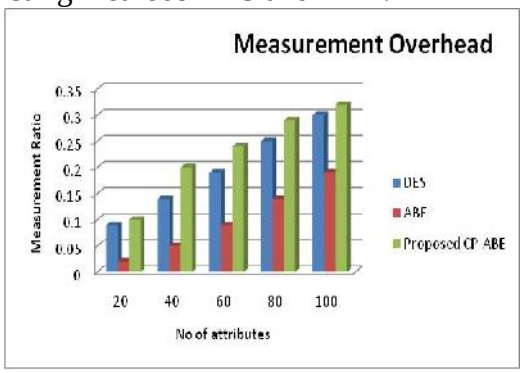

Figure 2: Comparison graph values of Measurement Overhead

Comparison graph (fig.2) explains the values of measurement over headed in two existing methods DES, ABE and one proposed method CP-ABE. The values of both the methods are measured by number of attributes from 20 to 100 and also by measuring the ratio. The ratio of measurement overhead in DES is 0.09 minimum and 0.3 maximum, in ABE the ratio measured is minimum 0.02 and 0.19 maximum and in proposed method CP-ABE the ratio measured is minimum 0.1 and maximum 0.32. It is assumed that the value of measurement over headed in Proposed method is high when compared to two existing methods DES and ABE.

Communication Overhead

DES	ABE	Proposed CP-ABE
0.73	0.41	0.8
0.73	0.47	0.83
0.83	0.53	0.85
0.78	0.55	0.89

Table 3: Comparison table values of Communication Overhead

Comparison table 3 explains the values of communication over head in two existing methods DES and ABE and one proposed method CP-ABE. The ratio of communication overhead in DES is 0.73 minimum and 0.78 maximum, in ABE the ratio measured is minimum 0.41 and 0.55 maximum and in proposed method CP-ABE the ratio measured is minimum 0.8 and maximum 0.89. It is assumed that the value of measurement over headed in Proposed method is high when compared to two existing methods DES and ABE.

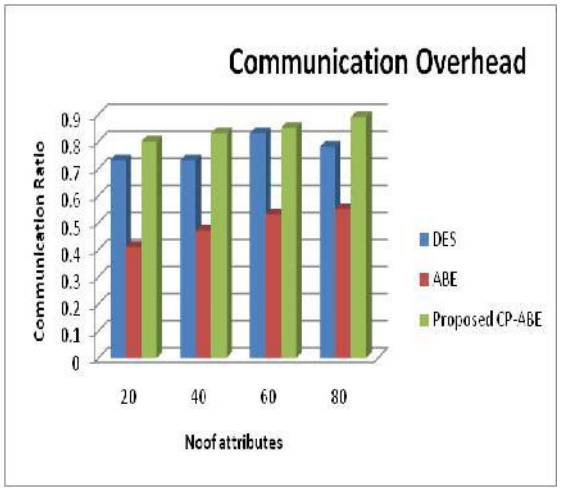

Figure 3: Comparison graph values of Communication Overhead

Comparison graph (fig.3) explains the values of communication over headed in two existing methods DES, ABE and one proposed method CP-ABE. The values of both the methods are measured by number of attributes from 20 to 80 and also by measuring the ratio The ratio of communication overhead in DES is 0.73 minimum and 0.78 maximum, in ABE the ratio measured is minimum 0.41 and 0.55 maximum and in proposed method CP-ABE the ratio measured is minimum 0.8 and maximum 0.89. It is assumed that the value of measurement of communication over headed in Proposed method is high when compared to two existing methods DES and ABE.

CONCLUSION

As of late, numerous examinations on get to manage in cloud depend on good encryption calculation (ABE). In any case, customary ABE isn't appropriate for portable cloud since it is computationally escalated and versatile gadgets just have restricted assets. In this rag, we suggest D-S-A to explain this matter. It presents a novel DSA-CP-ABE calculation to move significant calculation overhead from cell phones onto intermediary servers, following, it can fathom the protected data portion out issue in conveyable cloud. The trial comes to explain the DSA can guarantee information protection in portable cloud and diminish the over- head on clients' side in versatile cloud. Later on work, we will plan new ways to deal with guarantee information honesty. Additionally tap the capability of portable cloud, we will likewise ponder how to do ciphertext recovery over existing information sharing plans.

REFERENCES

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Hand-book of Applied Cryptography. CRC Press, August 2011 edition, 1996. Fifth Printing.

[2] Douglas R. Stinson. Cryptography: Theory and Practice. CRC Press, third November 2005) edition, 1995.

[3] Alex Biryukov, Adi Shamir, and David Wagner. Real time cryptanalysis of A5/1 on a PC. In Bruce Schneier, editor, FSE, volume 1978 of Lecture Notes in Computer Science, pages 1–18. Springer, 2000.

[4] Bluetooth T M. Bluetooth specification, v4.0, June 2010. E0 encryption algorithm described in volume 2, pages 1072–1081. Available online at http://www.bluetooth.org.

[5] Marc Briceno, Ian Goldberg, and David Wagner. A pedagogical implementation of the GSM A5/1 and A5/2 voice privacy‖

encryption algorithms. Available online at http://www.scard.org/gsm/a51.html, 1998.
[6] 3rd Generation Partnership Project. Specification of the 3GPP confidentiality and integrity algorithms UEA2 & UIA2. ETSI/SAGE Specification Document 2: SNOW 3G Specification, v1.1, September 6, 2006.
[7] ECRYPT Stream Cipher Project eSTREAM. The current eSTREAM portfolio. Available online at http://www.ecrypt.eu.org/stream/ index.html.
[8] ECRYPT Stream Cipher Project eSTREAM. Software performance results from the eSTREAM project. Available online at http://www. ecrypt.eu.org/stream/perf/#results.
[9] Ciphertext-Policy Attribute-Based Encryption Yanli Ren ; Shuozhong Wang ; Xinpeng Zhang ; Zhenxing Qian 2011 Third International Conference on Multimedia Information Networking and Security Year: 2011