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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Study of Control Cloud Data Access Privilege and Anonymity Based on Fully Anonymous Attribute Revocation

Dr. K. Praveen Kumar[1], K. Sree Ranganayaki[2]

Associate Professor, Department of Computing, School of Electrical Engineering & Computing, Adama Science &Technology University, Adama, Ethiopia[1]

M. Tech Student, Chaitanya Institute of Technology and Science, Warangal, India[2]

ABSTRACT: Cloud computing is a progressive computing paradigm, which permits bendy, on-demand, and low-cost utilization of computing assets, however the records is outsourced to a few cloud servers, and diverse privateness worries emerge from it. In this paper, we tried to present a privilege control scheme Anonymity Control to address and the user identification privateness in current access control. Anonymity Control decentralizes the important authority to restrict the identity leakage and for that reason achieves partial anonymity. It additionally generates the file get right of access to control to the privilege control, by way of which privileges of all operations on the cloud data can be controlled in a right manner. We present the Anonymity Control-F, which prevents the identification and obtain the anonymity.

KEYWORDS: Anonymity, multi-authority, attribute-basedencryption.

I. INTRODUCTION

Cloud Computing set up pervasive, convenient, on demand network get right of access to a shared pool of configurable computing resources (e.g., networks, servers, storage, programs, and services) that may be straight away provision and released with vital efforts for management or service provider interplay. Its major goal is to supply quick, relaxed, handy data storage and internet computing service, with all computing sources envision as offerings and delivered over the Internet. A quantity of computing concepts and technology are mixed in Cloud Computing to satisfy the computing needs of users, it offers common commercial enterprise programs on line over internet browsers, whilst their data and software's are stored on the servers. This is an approach that is used to maximize the scope or step up competencies robustly without making an investment in new infrastructure, sustenance new personnel or licensing new software. It affords quality storage for data and rapid computing to clients over the internet. Data safety is one of the components of the cloud which prohibit users from the usage of cloud offerings. There is distress between the data owner's mainly in huge agencies that their data probable misuse by the cloud company without their data. Data safety of the users can be ensured by the use of the idea of digital personal networks, firewalls, and by using enforcing different safety rules inside its very own circumferences.

Security is consequently an extensive element in any cloud computing surroundings, due to the fact it is important to guarantee that best authorized get right of access to is sanctioned and guarded behaviour Is normal. Any type of security and privateness contravention is important and can produce vital effects. As soon as the strict guidelines and policies are taken towards privacy in cloud, more and more employees will sense store to adopt cloud computing. A client can be individual or a big organization but all are having identical concern i.e. Records protection, so data security is dreadful effect. Data security at different ranges is the crucial matter of this generation; it is able to be labelled into categories: Security at External stage and Security at Internal Level. Security at External stage states that facts is unsecure hostile to third party auditor, cloud provider issuer or community intruder. Security at Internal degree states that facts are unsecure hostile to authorized clients or worker of an enterprise.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

A secure server plus provides a blanketed basis for web hosting our Web packages, and Web server configuration performs a crucial function for our Web software's protection. Badly configured server can result in unauthorized get right of access to. A forgotten percentage can provide a handy lower back door, at the same time as an omitted port may be an attacker's front door. Neglected user money owed can allow an attacker to slip by our defences unnoticed. Understanding threats to our Web server and being capable of discover appropriate countermeasures allows us to count on many attacks and thwart the ever growing numbers of attackers. This system affords bidirectional encryption of communications between a client and server, which protects in opposition to eavesdropping and tampering with and/or forging the contents of the communication. In exercise, this affords an affordable guarantee that one is communicating with precisely. The internet site that one meant to speak with, in addition to making sure that the contents of communications between the person and location cannot be examine or forged by any third party auditing.

II. RELATED WORK

There are numerous works carried in the area of data protection at cloud. Many models, schemes and strategies are proposed for data security. M. Sugumaran et al [10] illustrates multiple techniques that resolves the security of the data and proposes architecture to guard the statistics in cloud. In proposed structure the encrypted data is stored in cloud the use of cryptography approach i.e. Located on block cipher.

Cindhamani.J et al [3] proposed a stronger frame works for data security in cloud which follows the safety polices such as integrity, confidentiality and availability. Parameters they used are 128 bit encryption, RSA set of rules and Trusted PartyAuditor (TPA). Before storing the data into the cloud, the facts owner assigns the privileges that who will get access to the data. After assigning the privileges they encrypt the data and stores into the cloud.

Dharmendra [4] proposed the unified data encryption architecture which ensures the data security and privateness with affordable overall performance overhead of computing machine. It is based totally on multilevel identification encryption method with two degree/issue identification verification system.

Dr. L.Arockiam et al [5] achieves the data confidentiality in cloudstorage with exclusive strategies i.e. Encryption and obfuscation. Encryption encrypts the alpha-numeric and alpha facts while obfuscation encrypts the numeric statistics. Both are accomplished on user side. First, the user has to encrypt the data usingany approach then he stores the data into cloud garage. TaehoJung et al [14] use two schemes to govern the data privateness and the identification privateness. One is the Anony Control scheme i.e.Semianonymous privilege control scheme which not best addresses the data privacy but also the user identification privacy inextant access control schemes. It decentralizes the important authority to restraint the identity leakage and accordingly achieves semianonymity. Another is the AnonyControl-F scheme that controls the identity leakage and achieves the whole anonymity.

Eman M.Mohamed et al [6] Exhibits the data protection model that is based totally at the evaluation of cloud architecture and applied software to intensify enterprise in statistics security model for cloud computing. Hu Shuijing [7] defined the giant essentials in cloud computing, consisting of protection key era, regulation and preferred etc and discussed way in which they may be addressed. In this Proposed model data is covered in opposition to all threats i.e.Internal and external, thread all through, transits in addition to when information at rest.

III.ANONYCONTROL AND ANONYCONTROL-F

In this system [1], there are four types of entities: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers (refer Fig.1). A user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree T_p can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree T_p. To formally define the security of our Anony Control, we first give the following definitions.

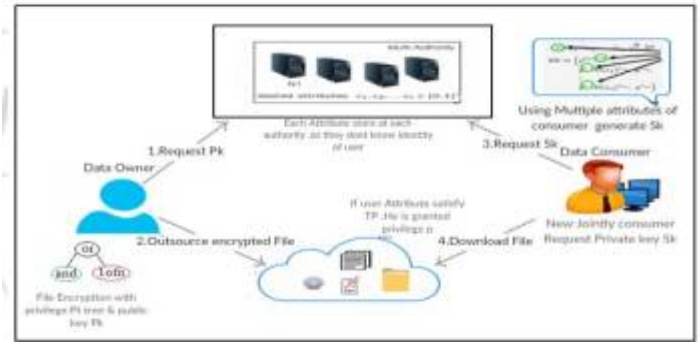

Figure 1: System Architecture

Setup→ PK, MK_k : This algorithm takes nothing as input except implicit inputs such as security parameters. Attributes authorities execute this algorithm to jointly compute asystem-wide public parameter PK as well as an authority wide public parameter y_k , and to individually compute amaster key MKk .

KeyGenerate (PK, MK_k, A_u) → SK_u: This algorithm enablesa user to interact with every attribute authority, and obtains aprivate key SK_u corresponding to the input attribute set Au.

Encrypt(PK, M, $\{T_p\}p\in\{0,...,r-1\}$) → (CT,VR): This algorithm takes as input the public key PK, a message M, anda set of privilege trees $\{Tp\}p\in\{0,...,r-1\}$, where r is determined by the encrypter. It will encrypt the message Mand returns a ciphertext CT and verification set VR so that auser can execute specific operation on the ciphertext if andonly if his attributes satisfy the corresponding privilege treeTp. As we defined, T0 stands for the privilege to read the file.
Decrypt (PK, SK_u , CT) → M or verification parameter: This algorithm will be used at file controlling (e.g. reading, modification, deletion). It takes as input the public key PK, aciphertext CT, and a private key SKu, which has a set of attributes A_u and corresponds to its holder's GID_u. If the setAu satisfies any tree in the set $\{Tp\}p\in\{0,..., r-1\}$, the algorithm returns a message M or a verification parameter. If the verification parameter is successfully verified by Cloud Servers, who use VR to verify it, the operation request will be processed.

As we studied various schemes of ABE like IBE, KP-ABE, CP-ABE also one access control system i.e AnonyControl but the common problem with this techniques that no author work on user revocation strategy with these techniques, because whenever we want to implement these techniques in real scenario then there will be a need of user revocation, sohere we proposed user revocation strategy which can work with AnonyControl system. In Revocational AnonyControl system after key generation phase, multi authority system build revocation tree R_t by using attributes of user. There vocation tree corresponds to time t and the identifier of revoked user is uid which is associated with one leaf node. So user uid is revoked only when there attributes matches with revocation tree R_t attribute set.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

IV. SUGGESTED WORK

Propose anonymity Control to allow cloud servers to control users' access privileges without knowing theiridentity information.
1. The proposed schemes are able to protect user's privacy against each single authority. Partial information isdisclosed in anonymity Control and no information is disclosed in anonymity Control-F.
2. The proposed schemes are tolerant against authority compromise, and compromising of up to (N −2) authoritiesdoes not bring the whole system down.
3. Provided detailed analysis on security and performance to show feasibility of the scheme anonymityControl and anonymity Control-F.
4. First implement the real toolkit of a multi-authority based encryption scheme anonymity Control and anonymityControl-F.

In this setting, each authority knows only a part of anyuser's attributes, which are not enough to figure out theuser's identity. However, the scheme proposed by Chaseconsidered the basic threshold-based KP-ABE, which lacks generality in the encryption policy expression. Many attribute based encryption schemes having multiple authorities have been proposed afterwards, but they either also employ a threshold-based ABE or have a semi-honestcentral authority, or cannot tolerate arbitrarily many users'collusion attack.

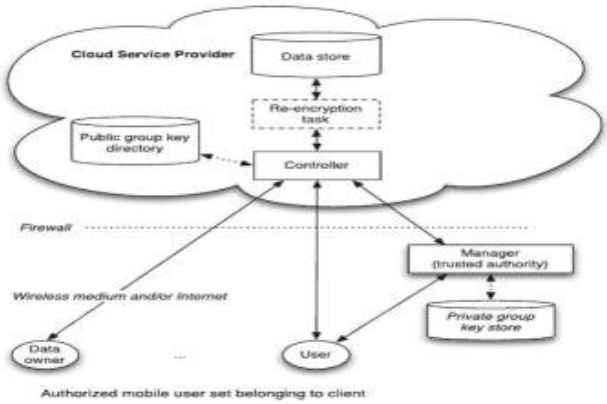

Figure 2: Suggested block diagram

Algorithm 1
1-Out-of-2 Oblivious Transfer
1: Bob randomly picks a secret s and publishes g_s to Alice.
2: Alice creates an encryption/decryption key pair :{g_r , r}
3: Alice chooses i and calculates $EK_i = g_r, Ek_{i-1} = g_s, g_r$and sends EK_0 to Bob.
4: Bob calculates $EK_1 = g_s\ EK_0$and encrypts M_0 using EK_0 and M_1using EK_1 and sends two cipher texts$EEK_0(M_0)$, $EEK_1(M_1)$ to Alice.
5: Alice can user to decrypt the desired cipher text$EEK_i(M_i)$, but she cannot decrypt the other one. Meanwhile,Bob does not know which cipher text is decrypted.

Algorithm 2
1-Out-of-n Oblivious Transfer
1: Bob randomly picks n secrets $S_1 \ldots\ldots\ldots\ldots\ldots S_n$and calculates $t_i$as follows:
$\forall i \in \{1, \ldots, n\} : t_i = S_1 \oplus \bullet \cdot\cdot \oplus S_{i-1} \oplus M_i$

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

2: For each i ∈ {1, . . . , n}, Bob and Alice are engaged ina 1-out-of-2 OT where Bob's first message is t_i and thesecond message is S_i. Alice picks t_i to receive if she wants M_i and S_i otherwise.
3: After Alice receives n components, she has $t_i = S_1 \oplus \bullet \cdot \cdot \oplus S_{i-1} \oplus M_i$ for the i she wants and $S_k$for k _= i , she canrecover the M_i byI. $M_i = t_i \oplus S_{i-1} \oplus S_{i-2} \cdot \cdot \oplus$s1

V. CONCLUSION

In this paper, the survey of various encryption schemes likeIBE, ABE, KP-ABE, CP-ABE, Anonycontrol and AnonyControl-F is noted with their advantage anddisadvantage. The unique variation of this scheme are compared and mentioned with the present scheme according to the upward thrust in the safety issues in cloud computing. Using multiple government inside the cloud computing machine, our suggested schemes attain no longer simplest quality-grained privilege manage however also identity anonymity while engaging in privilege manage based totally on users' identity data. More importantly, our device can tolerate upto N − 2 authority compromise, that is enormously most advantageous mainly in Internet-based cloud computing environment. We also carried out specific security and overall recital evaluation which suggests that Anony- Control both relaxed and efficient for cloud garage system.

REFERENCES

[1] Control Cloud Data Access Privilege and Anonymitywith Fully Anonymous Attribute-Based Encryption190 IEEE transactions on informationforensics and security, vol. 10, no. 1,January 2015
[2] A Privilege Based Attribute Encryption System ForSecure and Reliable Data Sharing. International Journalof Innovative Research in Computer andCommunication Engineering (An ISO 3297: 2007Certified Organization) Vol. 2, Issue 5, May 2014
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute based encryption," in Proc. IEEE SP,May 2007, pp. 321–334.
[4] A. Shamir, "Identity-based cryptosystems and signatureschemes," in Advances in Cryptology. Berlin, Germany:Springer-Verlag, 1985, pp. 47–53.
[5] A. Sahai and B. Waters, "Fuzzy identity-basedencryption," in Advances in Cryptology. Berlin,Germany: Springer-Verlag, 2005, pp. 457–473.
[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Attribute-based encryption for fine-grained accesscontrol of encrypted data," in Proc. 13th
[7] Identity-Based Encryption with Outsourced Revocationin Cloud Computing IEEE transactions oncomputers, vol. 64, no. 2, February 2015
[8] Improving Privacy and Security in DecentralizedCiphertext-Policy Attribute-Based Encryption JinguangHan, Member, IEEE, Willy Susilo, Senior Member,IEEE, Yi Mu, Senior Member, IEEE.
[9] Jianying Zhou, and Man Ho Allen Au, Member, IEEEK. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS:Effective data access control for multi-authority cloudstorage systems," in Proc. IEEE INFOCOM, Apr. 2013,pp. 2895–2903.
[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute baseddata sharing with attribute revocation," in Proc. 5thACM Symp. Inf. Comput. Commun. Security(ASIACCS'10), 2010, pp. 261–270

BIOGRAPHY

Dr.K.Praveen Kumar received the PhD in Computer Science & Engineering in 2015, M.Tech in Software Engineering from Kakatiya Institute of Technology & Science Warangal, Telangana, India in 2010 and B.Tech in Information Technology from Kakatiya Institute of Technology & Science Warangal, Telangana, India 2007. Presently working as Assistant Professor in Computer Science Department at Adama Science and Technology University, Adama, Ethiopia.

K Sree Ranganayaki pursuing M.Tech in Computer Science & Engineering at Chaitanya Institute of Technology and Science. Her Area of Interest is Network Science and Cloud Computing.