International Journal of Scientific Research in Computer Science, Engineering and Information Technology
 | Volume 3 | Issue 4 | ISSN : 2456-3307

Fine grained Access Control using Attribute-Based Encryption (ABE) Technique in Cloud Computing

N. Prudvi Kumar Reddy[1], Dr. E. Kesavulu Reddy[2]
PG Scholar, Department of Computer Science S.V.University, Tirupati, Andhra Pradesh, India

ABSTRACT

With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. 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. To guarantee confidentiality and proper access control of outsourced sensitive data, classical encryption techniques are used. However, such access control schemes are not feasible in cloud computing because of their lack of flexibility, scalability, and fine-grained access control. Instead, Attribute-Based Encryption (ABE) techniques are used in the cloud. This paper extensively surveys all ABE schemes and creates a comparison table for the key criteria for these schemes in cloud applications.

Keywords: Attribute-Based Encryption, Cloud Computing, Fine-Grained Access

I. INTRODUCTION

of users to store sensitive data on third party servers, either for cost saving or for simplicity of sharing. Cloud computing is now considered the fifth utility after gas, water, electricity, and telephony.

Attribute-Based Encryption (ABE) is newly invented public key cryptographic technique Cloud computing is becoming ubiquitous as it offers fast and efficient on-demand services for storage, network, hardware, and software through the internet. Cloud computing offers new facilities to enterprises, companies, and the general public, and provides lowcost computing infrastructure for IT-based solutions. Cloud computing is not new; organizations such as universities, research laboratories, and the military in developed countries have long used networks for communication, but the term cloud is more recent. Cloud computing is being increasingly offered on the web as web technology has become faster and more complex. It is now used by a large number that works in a oneto-many fashion and is also called fuzzy encryption. Public key encryption methods store encrypted data on third party servers, while distributing decryption keys to authorized users. However, there are many drawbacks to this. First, it is difficult to efficiently manage the distribution of secret keys to authorized users. Second, there is a lack of flexibility and scalability. Third, data owners must be online whenever encrypting or re-encrypting data, or distributing the secret keys. ABE minimizes the above limitations by reducing the communication overhead of the internet and increasing scalability, flexibility, and fine-grained access control for large scale systems.

II. ALGORITHM

ABE

ABE is a public key cryptography technique that uses one-to-many encryption. ABE uses attributes as identities for both encryption and decryption of data. The cipher text and a user's secret key depend on attributes. If the attributes of a user key match those of the cipher text, then decryption is allowed. For example, assume that there are three attributes fstd, fac, csg and that the threshold value is 2, then the private key will need at least two descriptive attributes to decrypt data. to provide fine-grained access control, flexibility, and scalability in access control mechanisms in the cloud. ABE uses a set of four algorithms: setup, key generation, encryption, and decryption. Its limitations are as follows:

(1) Lack of an express ability in the sense of a threshold value.
(2) Different categories of users create a computational overhead.

Key Policy ABE (KP-ABE)

KP-ABE was proposed as a modified form of basic ABE. Initially security parameters are setup to encrypt the message M and descriptive attribute S using PK to produce Cipher Text (CT), as shown in Algorithm 1. In KP-ABE decryption, a key is embedded with an access structure and CT is annotated. The decryption of the ciphe text is only possible if the attributes of the CT satisfy the access structure of the user's secret key In KP-ABE, a policy is assigned to users when the authority to create key and attributes is assigned to the cipher text during its creation. KP-ABE reduces the computational overhead in a cloud server by enabling the data owner to express the access structure.

Algorithm 1

Setup(security parameter) -> PK, MK
Encrypt(PK, M, S) -> CT
KeyGen(MK, A) -> D
Decrypt(CT, D_A) -> M if $S \in A$
$\perp$ otherwise

A = access structure D = secret key
S = descriptive attribute M = message

KP-ABE has the following limitations:

(1) A sender cannot decide who can decrypt the data.
(2) It is not suitable in certain applications like sophisticated broadcast encryption.
(3) It lacks flexibility and scalability.

Expressive Key Policy ABE (EKP-ABE)

EKP-ABE is an extension of KP-ABE in which non-monotonic access structures are used. A non-monotonic access structure contains negated attributes. It uses Monotonic Access structure and additional NOT gate. For example, CS AND Std NOT graduate means that a student of computer science but not graduate. EKP-ABE sets a more flexible access structure by adding a negative word in front of an attribute, meaning that a person who has such attributes cannot decrypt the data. The main limitation of EKP-ABE is that it requires many negative attributes that are not related to the encrypted data but may exist in the encrypted data (useless attributes). This may cause huge overheads.

Cipher text Policy ABE (CP-ABE)

CP-ABE is a reversed model of KP-ABE. It is another modified form of ABE. The CP-ABE access structure is linked with a cipher text while the decryption key is annotated with a set of descriptive attributes, as shown in Algorithm 3. Therefore, the roles of the decryption key and cipher text are switched with respect to key policy ABE. In this scheme, encryption specifies the monotonic access structure with a threshold value for relevant attributes.

Algorithm 2

Setup(security parameter) -> PK, MK
Encrypt(PK, M, S) -> CT
KeyGen(MK, $\tilde{A}$u) -> D
Decrypt(CT, D) -> M if $S \in \tilde{A}$u
$\perp$otherwise
$\tilde{A}$u = non monotonic access structure
D = secret key
S = descriptive attribute M = message

Cipher text Policy Attribute-Set-Based Encryption (CP-ASBE)

CP-ASBE is an extended form of CP-ABE, which, unlike existing CP-ABE schemes that use a monolithic set of user attributes in a key, uses a structure based on a recursive set of user attributes. In CP-ABE, a decryption key supports only a logically organized single set of attributes and to satisfy cipher text, users can use combination of all the attributes from single set issued in their key.

Algorithm 3

Setup(security parameter) -> PK, MK
Encrypt(PK, M, A) -> CT
KeyGen(MK, S) -> D
Decrypt(CT, D) -> M if $S \in A$,
$\perp$otherwise
A = access structure D = secret key
S = descriptive attribute M = message

III. CONCLUSION

ABE is a broadly utilized encryption system for get to control in distributed computing. The fundamental favorable position of ABE is that it gives clients access to more grounded encryption and permits key quality circulation. This paper has broke down a few distinctive ABE methods what's more, classes, and surveyed their usefulness and restrictions. We stretched out the overview to weighted property based encryption methods that perform better by offering fine-grained get to control. Based on its fine-grained get to control, adaptability, and versatility in distributed computing, we finish up thatWABE executes and also or superior to the next plans.

IV. REFERENCES

[1]. Hamblen J O, van Bekkum G M E.An embedded systems laboratory to support rapid prototyping of robotics and the Internet of Things.IEEE Trans Edu, 2013, 56: 121–128

[2]. Ning H, Hu S.Technology classification, industry, and education for future Internet of Things.Int J Commun Syst, 2012, 25: 1230–1241

[3]. He M.The evolution and future trends of technology and information sciences.In: Proceedings of WASE International Conference on Information Engineering (ICIE 2009), Taiyuan, 2009.11–15

[4]. Zhou T C, Lyu M R T, King I, et al.Learning to suggest questions in social media.Knowl Inf Syst, 2014: 1–28

[5]. Ning H, He W, Hu S, et al.Space-time registration for physical-cyber world mapping in Internet of Things.In: Proceedings of IEEE 12th International Conference on Computer and Information Technology (CIT2012), Chengdu, 2012.307–310

[6]. Balasubramaniam S, Kangasharju J.Realizing the Internet of Nano Things: challenges, solutions, and applications.Computer, 2013, 46: 62–68 25 Akyildiz I F, Jornet J M.The Internet of Nano-Things.IEEE Wirel Commun, 2010, 17: 58–63

[7]. Dowling P J, Miburn G J.Quantum technology: the second quantum revolution.Phil Trans Roy Soc A-Math Phy, 2003, 361: 1655–1674

[8]. D.R.Kuhn, E.J.Coyne, and T.R.Weil, "Adding Attributes to Role- Based Access Control," IEEE Computer, vol.43, no.6, pp.79-81, June 2010.

[9]. M.Li, S.Yu, K.Ren, and W.Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc.Sixth Int'l ICST Conf.Security and Privacy in

Comm.Networks (SecureComm),pp.89- 106, 2010.
[10]. S.Yu, C.Wang, K.Ren, and W.Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc.ACM Symp.Information, Computer and Comm.Security (ASIACCS), pp.261-270, 2010.
[11]. G.Wang, Q.Liu, and J.Wu, "Hierarchical AttributeBased Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc.17th ACM Conf.Computer and Comm.Security (CCS), pp.735-737, 2010.
[12]. F.Zhao, T.Nishide, and K.Sakurai, "Realizing FineGrained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc.Seventh Int'l Conf.Information Security Practice and Experience (ISPEC), pp.83-97, 2011.
[13]. A.Sahai and B.Waters, "Fuzzy Identity-Based Encryption," Proc.Ann.Int'l Conf.Advances in Cryptology (EUROCRYPT), pp.457-473, 2005.
[14]. M.Chase, "Multi-Authority Attribute Based Encryption," Proc.Fourth Conf.Theory of cryptography (TCC), pp.515-534, 2007.
[15]. S.Ruj, M.Stojmenovic, and A.Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp.Cluster, Cloud and Grid Computing, pp.556- 563, 2012.
[16]. S.Ruj, M.Stojmenovic, and A.Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp.Cluster, Cloud and Grid Computing, pp.556- 563, 2012.
[17]. C.Wang, Q.Wang, K.Ren, N.Cao, and W.Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans.Services Computing, vol.5, no.2, pp.220-232, Apr.- June 2012.

Author's Profile:

N. Prudvi Kumar Reddy received Bachelor of science (MSCs) degree from Yogi vemana university, Kadapa in the year of 2011-2014. Pursuing Master of Computer Applications from Sri Venkateswara University, Tirupati in the year of 2015-2018. Research interest in the field of Computer Science in the area of Cryptography-Network Security, Data Mining, Cloud Computing and Software Engineering.

Dr.E.Kesavulu Reddy, working as an Assistant Professor in Dept. of. Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati (AP)-India. Received Master of Computer Applications and Doctorate in Computer Science from S.V.University, Tirupati, Andhra Pradesh India. Also received Master of Philosophy in Computer Science from M.K. University, Madurai, Tamilnadu, India. One paper presented in WCECS2010, U.S.A and two papers published in WCE 2011 & 2012, London, U.K. Published eight papers in International and five in National Journals, also attending in Five International and six National conferences. Research interest in the field of Computer Science in the area of Elliptic Curve Cryptography-Network Security, Data Mining, Cloud Computing and Software Engineering.