International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Cloud Privilege of Access to Data and Anonymity with the Unknown Entirely Based Encryption to Control Characteristics

1.Kaveti Sai Teja
Sreyas Institute of Engineering & Technology,
2.Mrs.Joshi Padma Narasimhachari
HoD & Associate Professor
Sreyas Institute of Engineering & Technology,
3.Dr. N. Ravi Shankar,
Professor in CSE, Lakireddy Balreddy College of Engineering, Vijayawada
4.Dr. M. B. Raju,
Professor in CSE, KrishnaMurthy Institute of Engineering & Technology, Hyderabad

ABSTRACT:

Cloud computing is a model revolutionary computing, which enables flexible, on-demand, low-cost and use of computing resources, but outsourcing data sources to some cloud servers, and concerns about the privacy of different out of it. Various schemes have been proposed based on the existing encryption feature to secure cloud storage. However, most of the work on the privacy of the contents of the data and access control, while focusing less attention is being given to the control of the franchise and privacy of identity. In this paper, we provide semi-anonymous control scheme AnonyControl privilege to address not only on data privacy, but also the privacy of the user's identity in the access control list systems. Decentralizes AnonyControl central authority to limit the leakage of identity and thus achieves semianonymity. Besides, it also circulates in the file control access to the control of a franchise, which privileges to all processes on the cloud data can be managed through a fine-grained. Later, we offer AnonyControl-F, which completely prevents the leakage of identity and achieve non-disclosure of his full name. Our security analysis shows that both AnonyControl and AnonyControl-F is safe under the coherent decision Diffie-Hellman assumption, and evaluate the performance of our exhibits feasibility of our plans

INTRODUCTION:

Cloud Computing is the use of computing resources (hardware and software) that are

delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

EXISTING SYSTEM:

- Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it.
- Few years later, Fuzzy Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE).
- The work by Lewko *et al.* and Muller *et al.* are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones.
- Lewko *et al.* use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to boolean formula, while we inherit the flexibility of the access tree having threshold gates.
- Muller *et al.* also supports only Disjunctive Normal Form (DNF) in their encryption policy.

DISADVANTAGES OF EXISTING SYSTEM:

- The identity is authenticated based on his information for the purpose of access control (or privilege control in this paper).
- Preferably, any authority or server alone should not know any client's personal information.
- The users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes

considerable problems in implementation.

PROPOSED SYSTEM:

- The data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes.
- We propose AnonyControl and AnonyControl-Fallow cloud servers to control users' access privileges without knowing their identity information. In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. The scheme proposed by Chase et al. considered the basic threshold-based KP-ABE. Many attribute based encryption schemes having multiple authorities have been proposed afterwards.
- In our system, there are four types of entities: *N Attribute Authorities* (denoted as *A*), *Cloud Server*, *Data Owners* and *Data Consumers*. 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* is joint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

ADVANTAGES OF PROPOSED SYSTEM:

- The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in *AnonyControl* and no information is disclosed in *AnonyControl-F*.
- The proposed schemes are tolerant against authority compromise, and compromising of up to $(N-2)$ authorities does not bring the whole system down.
- We provide detailed analysis on security and performance to show

feasibility of the scheme *AnonyControl* and *AnonyControl-F*.

- We firstly implement the real toolkit of a multiauthority based encryption scheme *AnonyControl* and *AnonyControl-F*.

LITERATURE SURVEY:

Attribute-based encryption for fine-grained access control of encrypted data

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt.[1]

Improving privacy and security in multi-authority attribute-based encryption

Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor differ-ent sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user ob-tain keys for appropriate attributes from each authority be-fore decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted central author-ity (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted author-ities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users ' privacy by preventing the authorities from pooling their information on particular users,

thus making ABE more usable in practice.[1]

Secure threshold multi authority attribute based encryption without a central authority

An attribute based encryption scheme (ABE) is a cryptographic primitive in which every user is identified by a set of attributes, and some function of these attributes is used to determine the ability to decrypt each ciphertext. Chase proposed the first multi authority ABE scheme in TCC 2007 as an answer to an open problem presented by Sahai and Waters in EUROCRYPT 2005. However, her scheme needs a fully trusted central authority which can decrypt every ciphertext in the system. This central authority would endanger the whole system if it's corrupted. This paper presents a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time.The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme and be further extended to a proactive MA-ABE scheme.[2]

Multi-authority attribute-based encryption with honest-but-curious central authority

An attribute-based encryption scheme capable of handling multiple authorities was recently proposed by Chase. The scheme is built upon a single-authority attribute-based encryption scheme presented earlier by Sahai and Waters. Chase's construction uses a trusted central authority that is inherently capable of decrypting arbitrary ciphertexts created within the system. We present a multi-authority attribute-based encryption scheme in which only the set of recipients defined by the encrypting party can decrypt a corresponding ciphertext. The central authority is viewed as 'honest-but-curious': on the one hand, it honestly follows the protocol, and on the other hand, it is curious to decrypt arbitrary ciphertexts thus violating the intent of the encrypting party. The proposed

scheme, which like its predecessors relies on the Bilinear Diffie–Hellman assumption, has a complexity comparable to that of Chase's scheme. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority.[3]

Attribute-based secure data sharing with hidden policies in smart grid

Smart grid uses intelligent transmission and distribution networks to deliver electricity. It aims to improve the electric system's reliability, security, and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning. The smart grid systems use fine-grained power grid measurements to provide increased grid stability and reliability. Key to achieving this is securely sharing the measurements among grid entities over wide area networks. Typically, such sharing follows policies that depend on data generator and consumer preferences and on time-sensitive contexts. In smart grid, as well as the data, policies for sharing the data may be sensitive because they directly contain sensitive information, and reveal information about underlying data protected by the policy, or about the data owner or recipients. In this study, we propose an attribute-based data sharing scheme in smart grid. Not only the data but also the access policies are obfuscated in grid operators' point of view during the data sharing process. Thus, the data privacy and policy privacy are preserved in the proposed scheme. The access policy can be expressed with any arbitrary access formula. Thus, the expressiveness of the policy is enhanced. The security is also improved such that the unauthorized key generation center or the grid manage systems that store the data cannot decrypt the data to be shared. The computation overhead of recipients are also reduced by delegating most of the laborious decryption operations to the more powerful grid manage systems.[4]

CONCLUSION

This project proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user

privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information.We also conducted detailed security and performance analysis which shows that Anony- Control both secure and efficient for cloud storage system.

FUTURE ENHANCEMENT

The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes who support efficient user revocation is one of our future works.

REFERENCES:

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE SP, May 2007, pp. 321–334.