Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 10, October-2017

Identity based and attribute based cryptography overcoming the cloud security issue while outsourcing cloud data.

Pooja S. Naik (naikp9011@gmail.com), Prof. Vinod S. Agrawal (vinodagrawal73@gmail.com)

MCA DEPARTMENT JNEC AURANGABAD (M.S-431003)

Abstract **--** An extension of the cryptographic technique of identity-based encryption (IBE), our proposed ABE scheme can serve as the basis of an access-control architecture in which entities require no interaction with a trusted authority in order to gain access to sensitive data. Changing scenario of cryptography has led to a change in paradigm of from certificate based public keys and key rings to user-dependent keys which are based on identities of users or their attributes. This is termed as identity based cryptography or attribute based cryptography. Such encryption schemes are much relevant in current scenario of cloud computing and mobile computing where participation of user in transactions is partial, or user-based access control over an encrypted database is required. This paper presents a survey of identity based and attribute based cryptographic primitives. *Index term*—**cryptography, security, cloud computing.**

INTRODUCTION

In 1984, Shamir, of RSA notoriety, introduced the concept of identity-based cryptography[1].Its primary innovation was its use of user identity attributes, such as email addresses or phone numbers, instead of digital certificates, for encryption and signature verification. This feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing users' certificates. It also makes it much easier to provide cryptography to unprepared users, since messages may be encrypted for users before they interact with any system components. The main problem here is that for every application or system unique string identifier cannot exist. Rather users are generally identified by their attributes. Sahai et al proposed attribute based encryption (ABE) as a problem to this solution.[4]

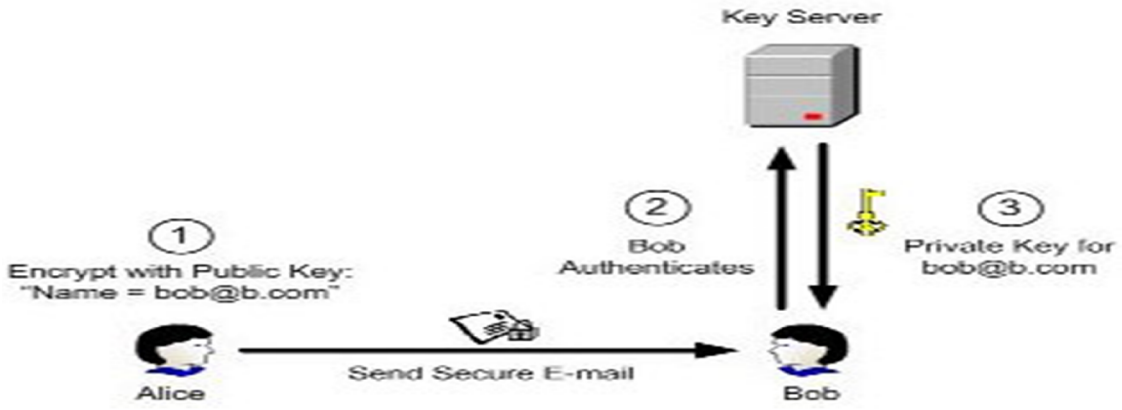
In a classical encryption scheme, for both the symmetric and asymmetric settings, a message is encrypted so that a single user, in possession of a secret key, can decrypt and recover the original plaintext. In the last years, other cryptographic paradigms have been proposed so that the sender of the message encrypts it in such a way that, later, many different users will be able to decrypt, as long as their identities, attributes or credentials are enough. In particular, maybe a user who is not registered in the system at the time where a message is encrypted can later decrypt it. Identity-based and attribute-based encryptions are perhaps the two instantiations of these alternative paradigms that have attracted more attention from the cryptographic community. These paradigms are suitable for situations where many different kinds of users and data are in place: social networks, the Internet of Things, Cloud storage and Cloud computation, analysis of big data, etc.In this paper we first review some important Identity based encryption, signature schemes. Subsequently, we review a few important attribute based encryption and signature schemes.[4]

I. IDENTITY BASED CRYPTOGRAPHY

Encryption keys derived from user identities are useful in avoiding trust problems which are generally faced in certificate based public key infrastructures (PKIs). This is so because there is no need of binding a public key to its owner, which is a single unique entity. These systems generally involve some trusted authorities, called private key generators, to compute users' private key from their identity information.

More concretely, an IBE system consists of four randomized algorithms, which we roughly summarize as follows: – setup: The function setup is executed by the PKG on input consisting of a security parameter k. The output includes parameters, a set of data comprising a message space, a cipher text space, and other parameters to be published by the PKG. Additionally, setup returns a private value master − key to be retained by the PKG, and used for generation of private decryption keys.[5]

- Key-gen: Given input parameters, master − key, and some string (public-key) ID, the function key-gen returns ID: the private key corresponding to ID.
- Encrypt: Given input parameters, the string (public-key) ID, and a message M, the function encrypt yields a cipher text C.
- Decrypt: Given input parameters, the string (public-key) ID, and the correct corresponding private key ID, the function decrypt returns the message M.



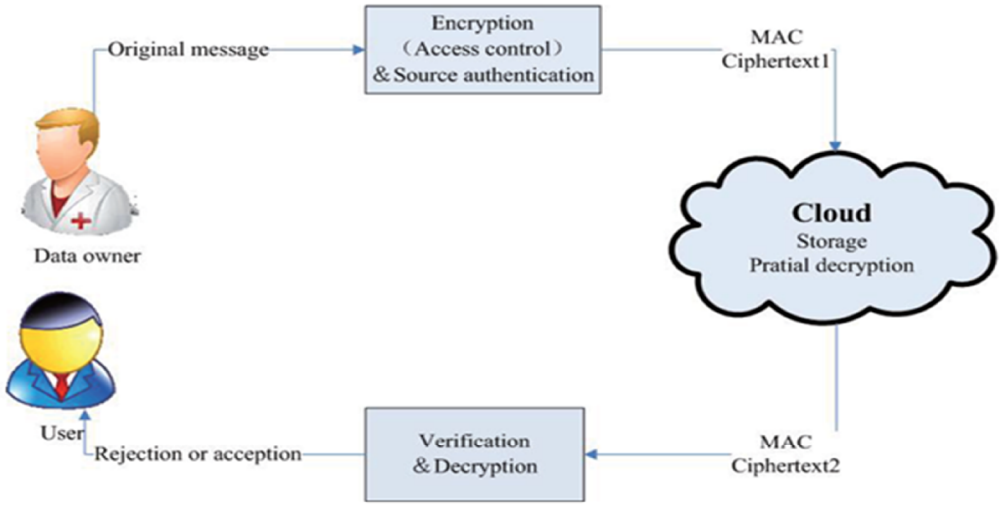
IDENTITY BASED CRYPTOGRAPHY

Secret sharing scheme –Secret sharing schemes are used to divide a secret among a number of parties. The information given to a party is called the share (of the secret) for that party. Every SSS realizes access structure that defines the sets of parties who should be able to reconstruct the secret by using their schemes. Shamir and Blakely were the first to propose a construction for secret-sharing schemes where the access structure is a threshold gate. That is, if any t or more parties come together, they can reconstruct the secret by using their shares. However, any lesser number of parties does not get any information about the secret.[4]

II.ATTRIBUTE BASED CRYPTOGRAPHY

Cloud users can also use cloud resources to perform complicated calculations. When utilizing cloud facilities, on the one side, cloud users want to keep their data safe and secret from other Internet users and even the service providers. On the other side, users may also need to gain more fine-grained control over their data, for example, how their data can be accessed.[2]

Having explained the mechanics of attribute certificates and IBE, we can now describe our ABE scheme. We describe two approaches with different security and use characteristics. The first, which we call identity-bound ABE, harmonizes with the more canonical use of attribute certificates as adjuncts to identity certificates. It has the drawback of requiring the transmitter of sensitive data to specify the identities of receivers in advance. The second approach, which we call freestanding ABE, makes use instead of freestanding attribute certificates as defined above. In other words, this latter approach treats attributes as distinct from the identity of their principal. A benefit of this feature is that access control policies may be specified without reference to the identities of principals. A drawback is the transferability of credentials, and the consequent difficult of attribute revocation. In both cases, the AA distributes IBE private keys corresponding to attribute strings; in other words, the AA serves as a PKG. In brief, an ABE system differs from a standard system employing attribute certificates in that the AA issues private keys to represent attributes, rather than signed statements or certificates.



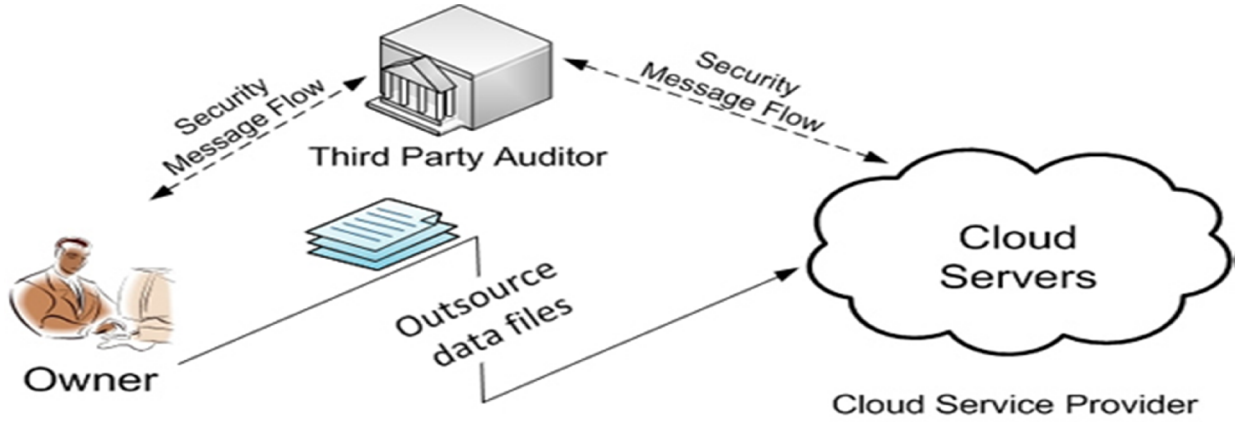
ATTRIBUTE BASED CRYPTOGRAPHY

The way how ABA proceeds can be summarized into the following steps:

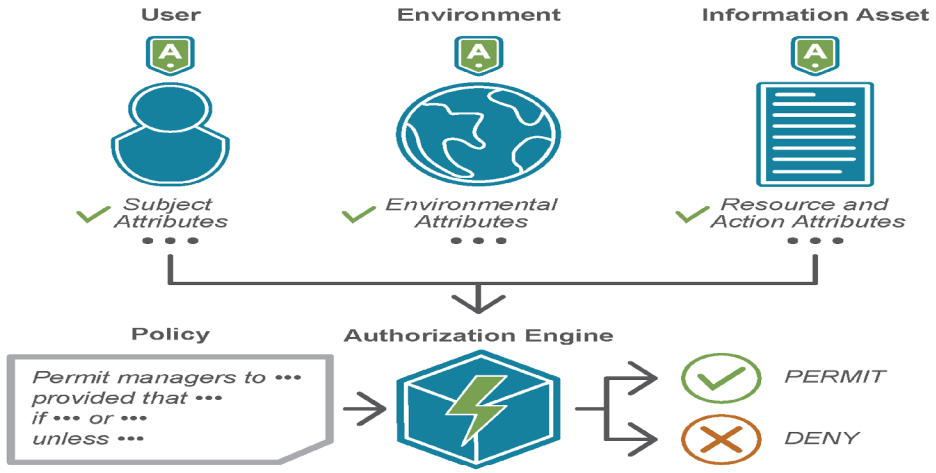
- A user obtains authorized attribute keys from the authority.
- 2. The user sends an authentication request to the authenticator.
- 3. After receiving the authentication request from the user, the authenticator responds with the attribute requirements.
- 4. If the user owns the required attributes, he or she generates a signature with the required attribute keys and sends the signature to the authenticator.
- 5. To verify the signature, the authenticator retrieves some information from the authority first, such as the user's attribute public keys, revocation information and so on. Next the authenticator checks whether the signature is valid or not.
- 6. The authenticator responses the user with the verification result, which is normally yes or no.

III.DATA OUTSOURCING

There is a top authority, which can only authorize new domain authorities. A domain authority can authorize both new domain authorities and data users. The top authority has the highest level of trust and the lowest level authorities have the lowest level of trust. In general, the lower the authorities are, the less trustful they are. data owners outsource their data in the cloud. At the same time, they want to have some control of the way how their data are accessed. Therefore, data owners define access requirements and the cloud server implements them. In addition, data users may want to access the data anonymously to the data owner. A possible solution can be based on ABAC (ATTRIBUTE BASED ACCESS CONTROL). First of all, data users register themselves to authorities and gain authorized credentials of the attributes they possess.



DATA OUTSOURCING BASED ON ABAC:-



IV. REVOCATION MECHANISMS

Revocation refers to authorizing a user key or the user itself. The associated problem is that when a user is removed, the attributes or the key might still remain valid and can be misused. Thus, in any multiuser encryption system we need mechanisms to deal with malicious users. The revocation mechanism of ABE schemes is more complicated than that of traditional public key cryptosystem or IBE schemes. The indirect revocation method implements revocation through an authority who releases a key update material periodically in such a way that only non-revoked users can update their keys. In this manner, the revoked users' keys automatically become invalid. The indirect method has an advantage that senders do not need to know the revocation list. A major drawback is that the key update phase, which requires periodic messages from the authority to all non-revoked users, can become a communication bottleneck.[4][5]

The direct revocation method enforces revocation directly by the sender who specifies the revocation list while encrypting the cipher text. A directly revocable KP-ABE scheme was first mentioned by Staddon et al., but their scheme only works when the number of attributes associated with a cipher text is exactly half of the size of the universe of real attributes. Attrapadung and Imai suggested a user-revocable ABE scheme by combining broadcast encryption schemes with ABE schemes. However, the data owner should take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation. This scheme is not applicable to the data outsourcing architecture, because the data owner will no longer be directly in control of data distribution after outsourcing their data to the external data server

V. CONCLUSION

Encryption mechanisms based on user identities and attributes hold a great promise for changing scenarios of computing, namely cloud computing and ubiquitous computing. These schemes relate a key with a set of attributes and thus alleviate the problem of key generation and distribution of PKI. Also, the concepts of such schemes can be used to further design trust and security mechanisms for data outsourcing in cloud.

REFERENCES

[1]A. Shamir. Identity-based cryptosystem and signature scheme. Proceedings of CRYPTO'84. Berlin: Springer, 1985, LNCS 196:47-53.
[2]A Sahai, B Waters. Fuzzy identity-based encryption. Proceedings of EUROCRYPT 2005. Berlin: Springer, 2005, LNCS 3494: 457-473.
[3]Attribute-Base Encryption Implies Identity-Based Encryption, JavierHerranz, Dept. Matem`atiques UniversitatPolit`ecnica de Catalunya c. JordiGirona 1-3, 08034, Barcelona, Spain.
[4]Identity Based and Attribute Based Cryptography: A Survey, Meenal Jain and Manoj Singh, ISSN-2348 –3733, Volume-2, Issue-5, May 2015
[5]Cryptographic Enforcement of Attribute based Authentication, Huihui Yang, University of Ander Faculty of Engineering and Science 2016[PDF]
[6]IDENTITY-BASED CHRYPTOGRAPHY: FROM PROPOSALS TO EVERYDAY USE, MihaiLica PURA, Victor Valeriu PATRICIU,INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER AFASES 2014 Brasov, 22-24 May 2014
[7]An Introduction to Identity-based Cryptography CSEP 590TU ▪ March 2005 ▪ Carl Youngblood [PDF]