Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 05, pp.31672-31675, May, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SECURED HASH ALGORITHM BASED ENCRYPTION TECHNIQUES

*Sharmila, M. and Dr. Pushparani, M.

Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Madurai Centre, India

ARTICLE INFO

Article History:
Received 23rd February, 2016
Received in revised form
05th March, 2016
Accepted 24th April, 2016
Published online 31st May, 2016

Key words:

Attributed based algorithm,
Secured hash algorithm,
Access control,
Authentication.

ABSTRACT

Attribute-based encryption (ABE) is a vision of public key encryption that allows users to encrypt and decrypt messages based on user attributes. In a typical implementation, the size of the ciphertext is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption. To reduce the decryption time in outsourced encryption method the user provides a transformation key to the cloud to translate any ABE ciphertext into simple ciphertext and it only incurs a small computational overhead for the user to recover the plaintext from the transformed ciphertext. We cannot guarantee that the cloud server will perform the transformation correctly. The proposed system introduces the Verifiable Outsourced Encryption so that the user can check the correctness of the transformation performed by the cloud server.

Citation: Sharmila, M. and Dr. Pushparani, M. 2016. "Secured hash algorithm based encryption techniques", *International Journal of Current Research*, 8, (05), 31672-31675.

INTRODUCTION

ABE (Attribute Based Encryption) is a new public key based one-to-many encryption that enables access control over encrypted data using access policies and ascribed attributes associated with private keys and cipher texts. There are two kinds of ABE schemes: key-policy ABE (KP-ABE) and cipher text-policy In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. In a KP-ABE scheme, the roles of an attribute set and an access policy are swapped from what we described for CP-ABE: attributes sets are used to annotate the cipher texts and access polices over these attributes are associated with users' private keys. In the policy, access structure and access formula interchangeably. The consequence of treating the patient based on incorrect information could be very serious or even catastrophic. The above observation motivates us to study ABE with verifiable outsourced decryption in this paper. We emphasize that an ABE scheme with secure outsourced decryption does not necessarily guarantee verifiability (i.e., correctness of the transformation done by the cloud server). For example, the secure ABE schemes with outsourced decryption proposed by Green et al. are not verifiable.

Literature Review

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. Method used here is Key-Policy Attribute-Based Encryption (KP-ABE). In this system cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Here cipher texts are associated with sets of attributes, whereas user secret keys are associated with policies.

Fully secure functional encryption

Attribute-based encryption and (hierarchical) inner product encryption. Previous constructions of ABE were only proven to be selectively secured not fully secure. The proposed system provides the fully secured encryption which overcomes the problem in the existing system Methods Used here is Dual system encryption. In a dual encryption system, keys and cipher texts can take on one of two forms normal and semi-functional A normal key can decrypt both normal and semi-functional ciphertexts. A semi-functional key can only decrypt normal cipher texts.

Provably secure cipher text policy ABE

This scheme allows an encryptor to use any AND gate on positive and negative attributes as an access policy on the

***Corresponding author: Sharmila, M.**
Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Madurai centre, India

cipher text. Methods Used here is cipher text policy attribute-based encryption. Proposed method to present variant with substantially smaller ciphertexts and faster encryption/decryption operations and to Obtain CCA security. In ciphertext policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every ciphertext is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the ciphertext access structure. This provides fine-grained access control on shared data in many practical settings, including secure databases and secure multicast.

Unbounded HIBE and Attribute-Based Encryption

In all previous constructions of HIBE in the standard model, a maximum hierarchy depth had to be xed at setup. In all previous constructions of ABE in the standard model, either a small universe size or a bound on the size of attribute sets had to be fixed at setup. A two-level HIBE (2-HIBE) scheme consists of a root private key generator (PKG), domain PKGs and users, all of which are associated with primitive IDs (PIDs) that are arbitrary strings. A user's public key consists of their PID and their domain's PID (in whole called an address). In a regular IBE (which corresponds to a 1-HIBE) scheme, there is only one PKG that distributes private keys to each user (whose public keys are their PID).In a 2-HIBE, users retrieve their private key from their domain PKG.Domain PKGs can compute the private key of any user in their domain, provided they have previously requested their domain secret key from the root PKG (who possesses a master secret).

Fuzzy identity-based encryption

The existing work in applying biometrics to cryptography has focused on the derivation of a secret from a biometric in a secret way. Biometric is used as an identity then the verification process for an identity is very clear. Biometric identity is an inherent trait and will always with a person. Using biometrics in Identity-Based Encryption will mean that the person will always have their public key handy. In several situations a user will want to present an encryption key to someone when they are physically present.

Existing System

In cipher text policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the cipher text access structure. Using (CP-ABE) any encryptor to specify access control in terms of any access formula over the attributes in the system. In the existing system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The Concept of verifiable is not descrbingin detail in the existing system. The introduced cipher text policy attribute based encryption is the new way for the encryption. The encryption is fully based on the user attributes. Most of the existing systems are proposed the attribute based encryption with various limitations and low performance to produce the cipher text. Whenever we use the attribute based encryption the length of the cipher text is greater to the proportion of the plain text size. There are many limitation some of them are: No error recovery algorithms are implemented in existing system. No methods to verify the transformation. Decryption time is high.

New cpa-abe scheme

In this section, we first propose a new CP-ABE scheme utilizing Waters' CP-ABE scheme, which is proven to be selectively CPA-secure. Then, based on the scheme, we proposea CP-ABE scheme with outsourced decryption and prove that it is selectively CPA-secure and verifiable in the standard model. Recently, the first CP-ABE scheme that achieved full security was proposed by Lewko *et al.* Since the underlying structure of the CP-ABE scheme presented by Lewko *et al)* is almost identical to the underlying Waters' CP-ABE scheme we use, one can adapt our construction techniques to the CP-ABE scheme proposed in to achieve fully secure (i.e., RCCA secure)CP-ABE scheme with verifiable outsourced decryption in, the standard model. This method can overcome many limitations, in that some of them are: The system let the user to verify the cloud server transformation. The proposed system is verifiable but not with compromised with security. It is a new approach for outsourcing encryption that user

New CP-ABE Scheme

Before presenting our new CP-ABE scheme, it gives some Intuitions of our construction. Based on Waters' CP-ABE Scheme [4], we add to the ciphertext the encryption of an extra random message and a checksum value, whichWe regard this checksum value as a commitment of the actual plaintext, which can be used to check if the transformation is done correctly in our CP-ABE Scheme with verifiable outsourced decryption. In fact, using our techniques, we can modify unbounded ABE schemes to unbounded ABE scheme with verifiable outsourced decryption.

CP-ABE scheme consists of the following algorithms:

Thus the cipher text-policy attribute based encryption scheme consists of four algorithms:

Setup

Encrypt

Key Generation

Decrypt

Setup (ƛ, U) The setup algorithm takes security parameter and attributes universe description as input. It outputs the public parameters (PK) and a master key (MK)

Encrypt (PK, M, A) The encryption algorithm takes as input the public parameters (PK), a message (M), and an access structure A. It outputs a cipher-text CT.

Key Generation (MK, S) The key generation algorithm takes as input the master key (MK) and a set of attributes (S) that describe the key. It outputs a private key (SK).

Decrypt(PK,CT,SK) The decryption algorithm takes as input the public parameters (PK), cipher text (CT), which contains an access policy (A), and a private key (SK), which is a private key for a set S of attributes. If the set (S) of attributes satisfies the access structure A then the algorithm decrypt the cipher text and return a message (M)

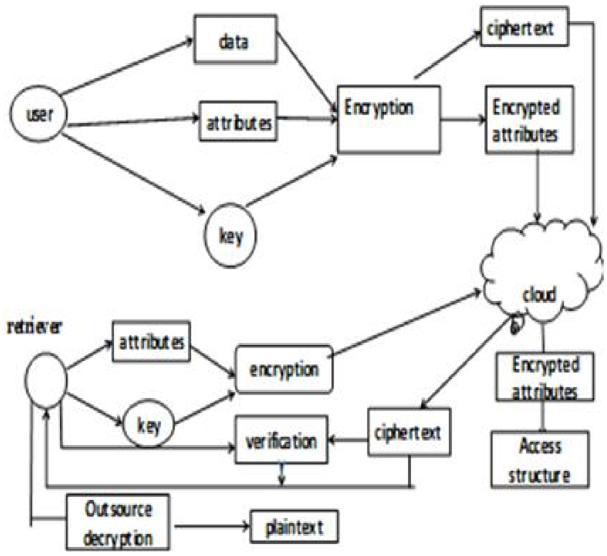


Fig. Key Process

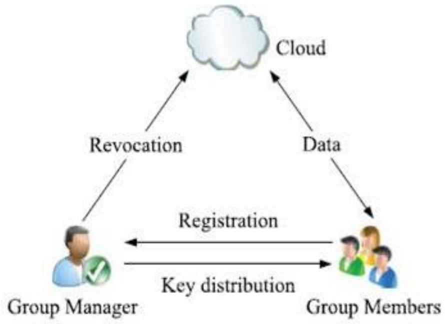


Fig. 1. System model

In ABE, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs. In Key-policy ABE or KP-ABE. (the sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes. In Cipher text-policy, CP-ABE. The receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates. All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase proposed a multi-authority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi-authority ABE protocol was studied in which required no trusted authority which requires every user to have attributes from at all the KDCs. Recently, Lewko and Waters .proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green *et* al proposed to outsource the decryption task to a proxy server, so that the user can computer with minimum resources (for example, hand held devices). However, the presence of one proxy and one key distribution center makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously. Presented a modification of authenticate users, who want to remain anonymous while accessing the clouds. To ensure anonymous user authentication Attribute Based Signatures were introduced. This was also a centralized approach. A recent scheme by the same authors .Takes a decentralized approach and provides authentication without disclosing the identity of the users. However, as mentioned earlier in the previous section it is prone to replay attack. The algorithm used:

Secure Hash Algorithm

Definition: SHA-1 is one of several cryptographic hash functions, most often used to verify that a file has been unaltered. SHA is short for Secure Hash Algorithm. File verification using SHA-1 is accomplished by comparing the checksums created after running the algorithm on the two files you want to compare. SHA-1 is the second iteration of this cryptographic hash function, replacing the previous SHA-0. An SHA-2 cryptographic hash function is also available and SHA-3 is being developed.

Encryption:

Let m be a message to be encrypted where m Zn. Select random r where r Z*n. Compute cipher text as: c= gm .rn mod n2.

Decryption:

Cipher text: cZ*n2.Compute message: m =L(cλ mod n2). M mod n Keys the files are encrypt with the public keys and set their Access policies (privileges).

File accesing:

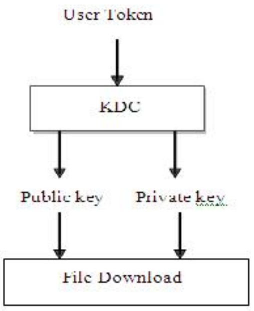


Fig. File Accessing

Analysis

This method satisfies the following requirements.

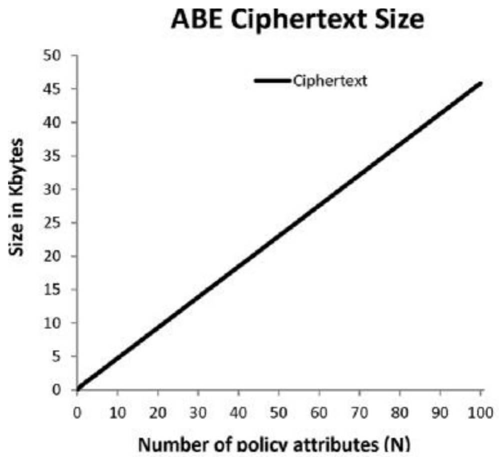
Confidentiality

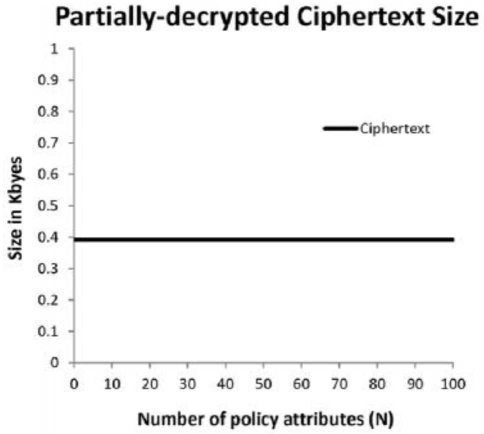
As the complexity of the pairing operation increases, it will be very difficult for the malicious third party to read or hack the encrypted content even thought eavesdrop on communication between the client and the sever.

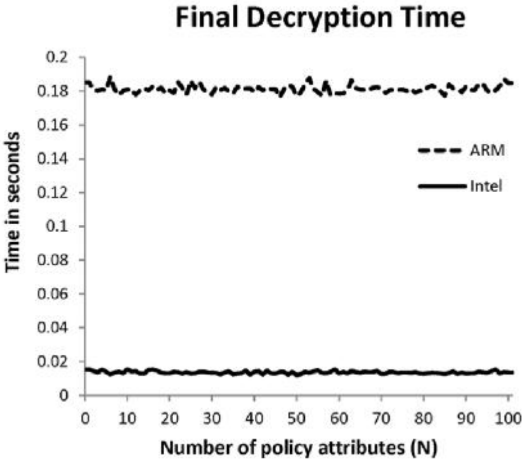
Authentication: As the document owner's attributes is used as the private key to encrypt the data which also server's as partial digital signature, as and when the data is decrypted by the data owner, he will be satisfied with the content as he has used his own attribute to encrypt it.

Verifiability: Check sum is widely used to verify whether the content that is encrypted and the content that is been received by the data owner is same.

Performance Evaluation: In order to evaluate the performance of CP-ABE scheme with verifiable outsourced decryption is presented in the below figures.







RESULTS

To provide Usage of High security cryptographic Using Blowfish algorithm, which is 448 bits key length results in higher security, rather than using traditional DES and AES algorithms are smaller in key sizes results in lesser security. Data Integrity Checking. It helps to ensure the data owner's data being stored in the cloud is valid or not. Data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research are yet to be identified in future

Conclusion

CP-ABE considered a new requirement of Abe with outsourced decryption: verifiability. By modified the original model of Abe with outsourced decryption proposed by green et al to include verifiability and by concrete on Abe scheme with verifiable outsourced decryption and proved that it is secure and verifiable. This proposed system scheme does not rely on random oracles. To assess the practicability of our scheme, model implemented it and conducted experiments in a simulated outsourcing environment. As expected, the scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.

REFERENCES

Attrapadung, J. Hernanz, F. Laguillaumie, B. Libert, E. DE Panfieu, and C. Rafols, 2012. "attribute-based encryption schemes with constant-size ciphertexts," theor. comput. sci., vol. 422, pp. 15–38.

Bethencourt, J., A. Sahai, and B. Waters, 2007. "ciphertext-policy attributebased encryption," in proc. ieee symp. security and privacy, pp. 321–334.

Cheung, L. and Cnewport, C. 2007. "provably secure ciphertext policy abe," in proc. acm conf. computer and communications security, pp. 456–465. 10 n.

Goyal, V. Pandey, O. Sahai, A. and Waters, B. 2006. "attribute-based encryption for fine-grained access control of encrypted data," in proc. acm conf. computer and communications security, pp. 89–98.

Lewko, A. B. and Waters, B. 2011. "unbounded hibe and attribute-based encryption," in proc. eurocrypt, pp. 547–567.

Lewko, A., Okamato, T. Sahai, A., K. Takashima, and B. Waters, 2010. "fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in proc. eurocrypt, pp. 62–91.

Okamato, T. and K. Takashima, 2010. "fully secure functional encryption with general relations from the decisional linear assumption," in proc. crypto, pp. 191–208.

Ostrovsky, R., Sahai, A. and Waters, B. 2007. "attribute-based encryption with non-monotonic access structures," in proc. acm conf. computer and communications security, pp. 195–203.

Sahai, A. and Waters, B. 2005. "fuzzy identity-based encryption," in proc. eurocrypt, pp. 457–473.

Waters, B. 2011. "ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in proc. public key cryptography, pp. 53–70.

****