Revisiting Attribute-Based Encryption with Verifiable Outsourced Decryption

Prof. Mrs. Jagruti A. Dandge,Ashwini M. Ambekar,Hemant P. Kadam,Sagar D. Kadve,Mayur V. Shinde

[1]Prof. Mrs. Jagruti A. Dandge Asst. Professor, Information Technology, PVG,COE,Nashik,Maharashtra,India
[2] Ashwini M. Ambekar BEIT, Information Technology, PVG, COE,Nashik,Maharashtra,India.
[3] Hemant P. Kadam BEIT, Information Technology, PVG, COE,Nashik,Maharashtra,India.
[4] Sagar D. Kadve BEIT, Information Technology, PVG, COE,Nashik,Maharashtra,India.
[5]Mayur V. Shinde BEIT, Information Technology, PVG, COE,Nashik,Maharashtra,India.

ABSTRACT

In this project main concept is to keep the data security and privacy for data owners is concern, the sharing data needs to be encrypted before being uploaded and fine grained access control is required. Attribute-based encryption (ABE) was thus proposed to have flexible Access control of encrypted data utilizing access policies and Attribute-based encryption (ABE) is a promising technique for fine grained access control of encrypted data in cloud storage, however, decryption involved in ABEs is usually too expensive for resource constrained front-end users, which greatly hinders its practical popularity. In order to reduce the decryption overhead for a user to recover the plain text, suggested the majority of the decryption work without revealing actually data or private keys. To ensure the third-party service honestly computes the outsourced work, provided a requirement of verifiability to the decryption of ABE, but their scheme doubled the size of the underlying ABE cipher text and the computation costs. Roughly speaking, their main idea is to use a parallel encryption technique, while one of the encryption components is used for the verification purpose. Hence the bandwidth and the computation cost are doubled. In that way propose a more efficient and generic construction of ABE with verifiable outsourced decryption (VO-ABE) based on an attribute-based key encapsulation mechanism (AB-KEM), a symmetric-key encryption scheme and a commitment scheme. Then in that, prove the security and the verification soundness of constructed ABE scheme in the standard model. Finally, instantiate this scheme with concrete building blocks. This scheme reduces the bandwidth and the computation costs almost by half. In this way prove that this system constructed ABE scheme is secure and meets the verification soundness in the standard model if the underlying building blocks are secure.

Keywords: - *encryption, decryption, verifiability, symmetric key*

1. Introduction

Now-a-days with the rapid development of cloud computing, growing data is being centralized into the cloud for sharing. To keep the data security and privacy for data owners, the sharing data needs to be encrypted before being uploaded and fine-grained access control is required. Attribute-based encryption (ABE) was thus proposed to have flexible Access control of encrypted data utilizing access policies and Attribute-based encryption (ABE) is a promising technique for fine-grained access control of encrypted data in cloud storage, however, decryption involved in ABEs is usually too expensive for resource-constrained front-end users, which greatly hinders its practical popularity [1]. In order to reduce the decryption overhead for a user to recover the plaintext suggested to outsource the majority of the decryption work without revealing actually data or private keys. To ensure the third-party service honestly computes the outsourced work, provided a requirement of verifiability to the decryption of ABE, but their scheme doubled the size of the underlying ABE cipher text and the computation costs. Roughly speaking, their main idea is to use a parallel encryption technique, while one of the encryption components is used for the verification purpose [2]. Hence the bandwidth and the computation cost are doubled. In this paper, we investigate the same problem. In particular, we propose a more efficient and generic construction of ABE with verifiable outsourced decryption (VO-ABE) based on an attribute-based key encapsulation mechanism (AB-KEM), a symmetric-key encryption scheme and a commitment scheme [3]. Then we prove the security and the verification soundness of our constructed ABE scheme in the standard model. Finally, we instantiate this scheme with concrete building blocks. This scheme reduces the bandwidth and the computation costs almost by half. We prove that our constructed ABE scheme is secure and meets the verification soundness in the standard model if the underlying building blocks are secure.

1.1 Encryption

Encryption is the process of encoding messages or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher-text that can only be read if decrypted.

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security aspect of Attribute-Based Encryption is

Collusion resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

1.2 Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Decryption involved in the ABEs is usually too expensive for resource-constrained front end users, which greatly hinders its practical popularity. In order to reduce the decryption overhead for a user to recover the plaintext suggested to outsource the majority of the decryption work without revealing actually data or private keys. It would be a significant challenge for users to complete the decryption independently on resources constrained devices. They proposed a key blinding technique to outsource the decryption without leaking data or secret keys as a precaution against maliciously detecting from the user service.

2. System Design

2.1 System Architecture

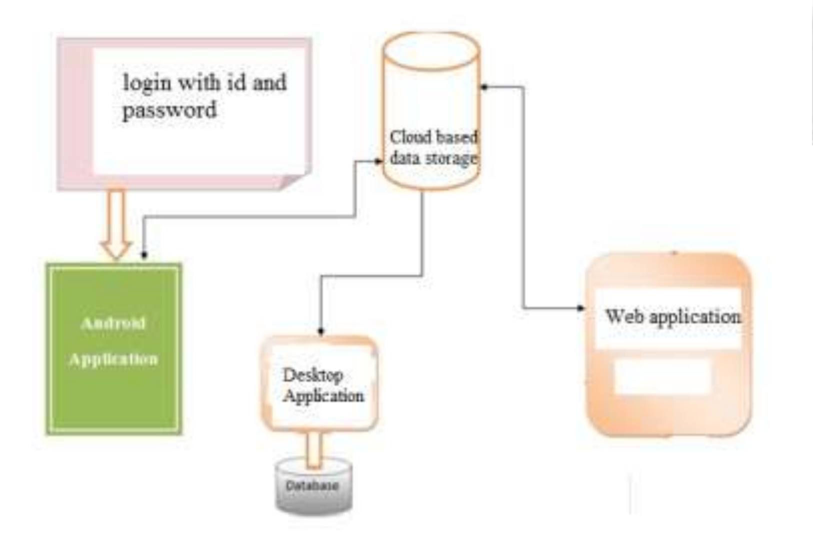
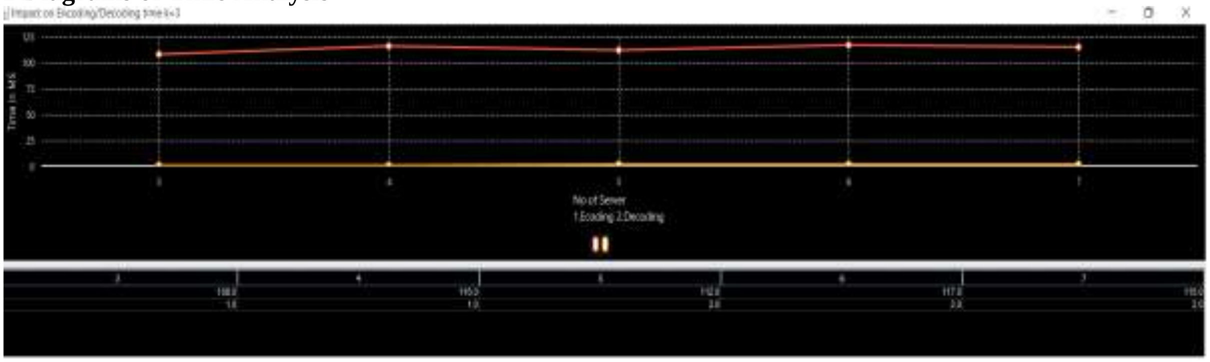


Fig 2.1: Process Overview Block Diagram

In above block diagram shows an ABE with verifiable outsourced decryption (VO-ABE) based on an AB KEM, a symmetric-key encryption scheme and a commitment scheme. In this provide a unified model of VO - ABE, which can be considered in both key-policy (KP) and cipher text-policy (CP) settings. Introduce verification to the outsourced decryption of ABE by adding an extra instance in the encryption/decryption algorithms, which duplicates the computation and communication overhead. Instead of two parallel instances in the encryption/decryption algorithms, combine a hybrid encryption and a commitment together to bundle the randomness to the cipher text, so that one can verify the outsourced computation easily [4]. Decryption is done in the natural way, but note that the outsourced transform key is obtained by an appropriate transform of the actual secret key with specific properties ensuring secure outsourced computation. In this approach define a verification algorithm for the data receiver to check the correctness of the outsourced computation.

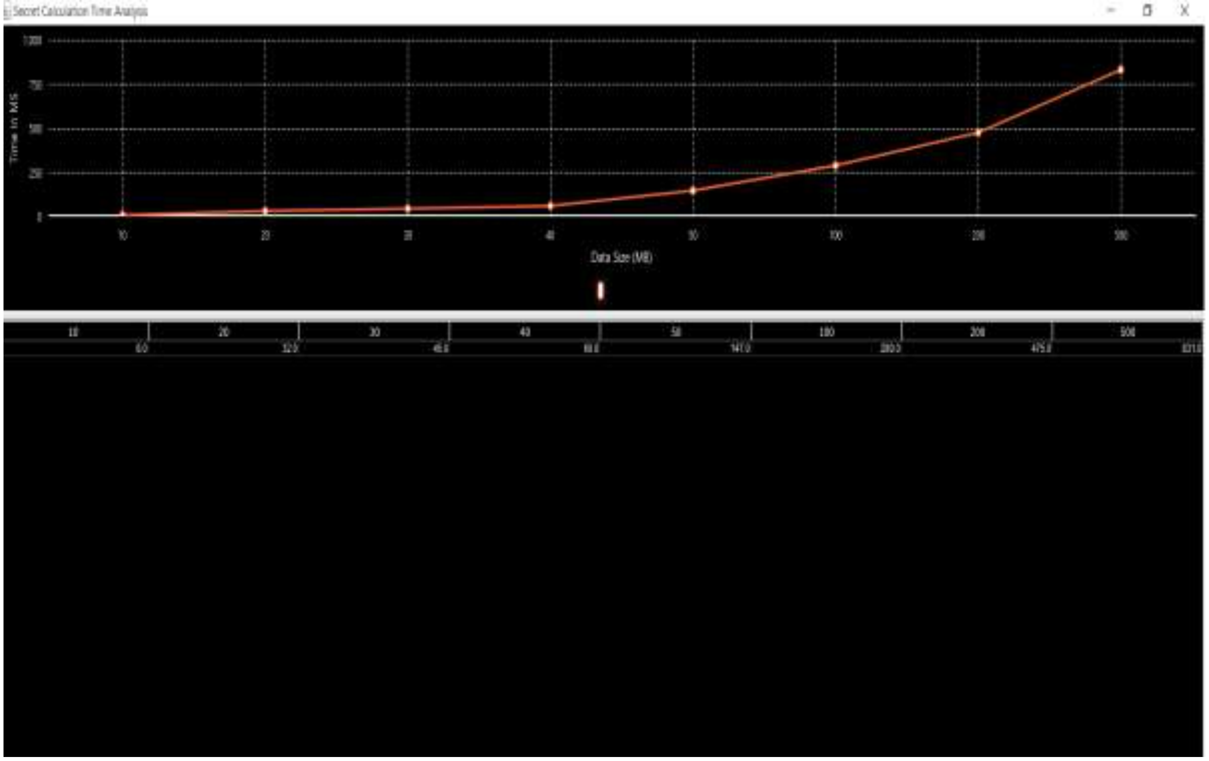
3. Time Analysis

3.1 Diagrams of Time Analysis



3	4	5	6	7
108.0	115.0	112.0	117.0	115.0
1.0	1.0	2.0	2.0	2.0

Fig 3.1: Search Time Analysis



10	20	30	40	50	100	200	500
6.0	32.0	46.0	68.0	141.0	280.0	475.0	831.0

Fig 3.2: Secret Calculation Time Analysis

4. CONCLUSIONS

The encryption time and the size of a standard ABE cipher text of this scheme are far less than specifically, a message encrypted under a policy with 100 attributes needs around 1 second and the size of the generated cipher text is around 16.68 KB, which are both nearly half of the counterparts and the third-party service for this scheme just needs half of the time used in to transform a standard ABE cipher text. The final decryption time is slightly more than half of that in. Therefore, In this way conclude that instantiation of ABE with verifiable outsourced decryption is more efficient than the existing scheme.

5. ACKNOWLEDGEMENT

Deep sense of gratitude towards our respected guide Prof. Mrs. J. A. Dandge for her valuable guidance, profound advice, persistent encouragement and help during the completion of this work. Her time to time helpful suggestions boosted us to complete this task successfully. She has helped us in all possible ways right from gathering the materials to report preparation. We extend our sincere thanks to Our Head of Department Prof. S. N. Bhadane,for providing all kinds of cooperation during the course. Our sincere thanks the Principal Dr. N. S. Walimbe for his inspiration. Finally we are thankful to the supporting staff of Information Technology department and all those who directly or indirectly contributed to complete this work.

6. REFERENCES

[1].A. Sahai and B. Waters, “*Fuzzy identity-based encryption*,” in Proc. EUROCRYPT, 2005, pp. 457–473.

[2]. M. Green, S. Hohenberger, and B. Waters, “*Outsourcing the decryption of abe ciphertexts*,” in Proc. USENIX Security Symp., 2011.

[3]. J. Lai, R. H. Deng, C. Guan, and J. Weng, “*Attributebased encryption with verifiable outsourced decryption,”*IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 13431354, 2013.

[4]. J. Bethencourt, A. Sahai, and B. Waters, “*Cipher text policy attribute-based encryption,*” in Proc. IEEE Symp.Security and Privacy, 2007, pp. 321–334.