Secured ABE Systems with Verifiable Outsourced Decryption

Vrince Vimal,
Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002,

Abstract
There is a tendency for private user information to be kept online by unauthorised parties. Attribute-based encryption (ABE) is a technique that may be used for encrypting logs. An individual log can be encrypted with characteristics that match the recipient's attributes rather than encrypting every piece of the log with all recipients' keys. In order to employ fewer keys, broadcast encryption may also be performed using this primitive. There will be a need to encrypt data saved at third-party websites as more sensitive data is exchanged and kept online by these websites. In this research, the system suggests basic designs of CPA-secure with RCCA-secure ABE systems in accordance with CPA-secure ABE with external decryption with reliable external decryption. The foundation of any type of ABE scheme is a CPA secure ABE system since it uses verifiable outsourced decryption, according to the system's high-level design. Additionally, the system instantiates our CPA-secure structure in the reference model before demonstrating how it was implemented. In this CPA-secure design, instead of independently encrypting an additional random message & implementing it to adhere to the real messagee, the message also a random value are encrypted simultaneously, and the message is committed to using the random value. Our scheme is more general, requires less processing, and produces smaller ciphertext. Additionally, it helps us more naturally acquire general RCCA-secure construction.

Keywords: Secured ABE System, Unauthorized Parties, Verifiable Outsourced Decryption, CPA-Secure, RCCA-Secure.

DOINumber: 10.48047/nq.2021.19.7.NQ21125 **NeuroQuantology2021;19(7):369-374**

1. INTRODUCTION
On the Internet, it's becoming more common for third parties to keep private user information. Personal information like email, data, as well as preferences are kept on online portals like Google and Yahoo. The attack correlation centre, dshield.org, maintains user-submitted intrusion reports in addition to providing aggregated views of Internet attacks. There is reason to worry that sensitive information will be stolen given the diversity, volume, and relevance of the information held at these sites. The current spike in assaults and the legal pressure these services are under have increased this concern.

A user can transfer data safely via encryption over an unsecure network or storage location. Earlier than the invention of public key cryptography, it was commonly believed that two users would need to create a secret key k that they both owned in order to communicate privately. While this could work for certain tiny or close-knit organisations, it was obviously impractical for bigger networks, like the Internet of today, which has billions of members. Diffie and Hellman created public key cryptography more than 30 years ago, and it is a concept that is still used today [DH76a, DH76b], safe communication between two parties is possible despite sharing a previous shared secret, fundamentally upending the received knowledge at the time.

Today, public key encryption is a priceless instrument whose usage is pervasive in the development of technologies for secure online communication (such as SSH, SSL), disc encryption, and the delivery of secure software patches. However, there is a pervasive misconception that (1) encryption is a way to send data or messages to a single person who holds the secret key and (2) Having data encryption access is either all or none, meaning that either the data can

be fully decrypted and read or only its length can be ascertained.

This idea of public-key encryption is inadequate for many new uses, such as "cloud" services. For instance, it's frequently necessary to provide a decryption policy in the ciphertext that can only be used by those who satisfy the requirements. More broadly, depending on the decryptor's authority, we could only wish to grant access to a certain function of the plaintext. Consider a cloud service that stores encrypted photos as a specific illustration. It could be necessary for law enforcement to ask the cloud to look for pictures with a specific face. As a result, the cloud requires a limited secret key that can only be used to decode pictures of the target face and not for anything else. In a broader sense, the secret key could only show a specific aspect of the plaintext picture, like a faceless target in a hazy image. For such applications, conventional public-key cryptography is ineffective.

With increasing access policy complexity, the amount of the ciphertext and decryption burden (computational cost) grows, which is one of the fundamental efficiency problems in the majority of present ABE methods. This turns into a major obstacle for programmes operating on devices with low resources. To encrypt its development projects, As an illustration, the college employs a pairing-based ABE method then uploads the ABE ciphertext that was produced to the university cloud.On a business ship, an authorised university administrative officer wishes to use his (resource-constrained) cell phone to check up the college's encrypted development initiatives. The ABE ciphertext is then desired to be downloaded and decrypted.

Because the pairing procedures required by the decryption approach are sometimes expensive for a device with low resources, he must wait a long time as well as sometimes eventually aborts the procedure for decryption. ABE system that uses external decryption. To be more precise, two keys are created for a user using a modified key generation process in their ABE system with external decryption. Initially, there is a short secret key of the El Gamal type that must be kept a secret by the user and is commonly referred to as the retrieving key rk. The second is the equivalent transformation key, often known as the tk key or the tk for short, which is shared with a proxy that is capable of being made public. In simple terms, this key pair is created via a key blinding approach. While the proxy acquires a ciphertext using the CP-ABE (or KP-ABE) algorithm for an attributes set or access policy, where the attributes set (or access policy) corresponding to the user meets the requirements, It may change the ABE ciphertext into a concise, straightforward El Gamal-style ciphertext using the transformation key, which decrypts to the same message. After that, the user just needs one exponentiation to decrypt this simple ciphertext after obtaining this brief and partially encrypted ciphertext.

In addition to the previous ABE approaches, Green et al. suggested two ABE methods with externalised decryption that, when subjected to chosen-plaintext attacks, are selectively CPA-secure. These two selectively CPA-secure ABE schemes with external decryption are further transformed into two selectively RCCA-secure ABE strategies in the random oracle architecture by using the Fujisaki-Okamoto transformation. Log encryption is possible using attribute-based encryption (ABE).The system in this study suggests general designs of CPA-secure as well as Verifiable outsourced decryption is used in RCCA-secure ABE systems that are developed by CPA-secure ABE. Additionally, it helps us more naturally acquire general RCCA-secure construction.

2. LITERATURE SURVEY

Trapdoor issues like the Decisional Diffie-Hellman (DDH) assumption are the foundation of cryptography. The attribute-based encryption method described in this work allows users to decode ciphertext encrypted with characteristics 0 if and only if they have at least k common components in common. They combined two intriguing technologies to create their scheme: bilinear maps, which add a new dimension to the DDH problem, and a novel trapdoor provided by a technique to disclose a secret in exponent. The attribute-based threshold strategy proposed a secret sharing mechanism utilising Lagrange's interpolation. An identity-based encryption was proposed as a solution to this issue, linking the polynomials intron sequel to the users.The Fuzzy IBE Scheme is a novel kind of IBE that takes into consideration a predetermined overlap distance measure and has uses in biometrics and document exchange on insecure servers. Because hostile users cannot cross their keys to decipher, it is protected from collusion attacks [1].

A user can share data over an unsafe network or storage location using functional encryption. It supports limited secret keys, which allow the owner of a key to only understand one specific function of encrypted data. This study examines the idea of functional encryption, which permits the generation of a key skk by a master secret key-holding authority to allow the computing of the function F(k, •) on encrypted data. The objective is to demonstrate that the definition cannot be met and to express the notion that the adversary only

discovers F(k, •) functions of the plaintext for which he is in possession of a secret key and learns nothing else about the plaintext.Bilinear maps are used in the inner product construction, and the "bi" in bilinear maps prevents going beyond inner products. Other methods, maybe taking inspiration from completely homomorphic encryption, could result in a broader category of predicates. Over an unsecured network, a user can safely communicate data. The fact that the secret key could only expose a function of the plaintext is a drawback [2].

The development of an innovative cryptosystem termed Key-Policy Attribute-Based Encryption (KP-ABE) enabling fine-grained exchange of encrypted data is the most crucial information in this article. To limit which ciphertexts a user may decode, this cryptosystem employs ciphertexts labelled with sets of characteristics along with private keys linked to access structures. It facilitates the delegation of private keys and is relevant to the exchange of audit-log information along with broadcast encryption. Attributed-Based Encryption (ABE) is a concept that Sahai and Waters introduced. According to ABE, ciphertexts and user keys are each labelled with a set of descriptive attributes, along with a key is able to decrypt a specific ciphertext if its attributes match the user's key.When creating a public/private key pair for a one-time signature scheme, an encyrptor will choose a set of criteria to use to encrypt the message in order to achieve CCA-2 security [3].

A new paradigm in computing called cloud computing allows for the delivery of IT resources and capabilities as Internet-based services while maintaining platform & deployment specifics hidden. To address this issue, a safe outsourcing methods into ABE has been introduced as a general and effective way to create attribute-based access control systems. We establish two cloud service providers (CSPs) to handle the users' as well as attribute authority's respective outsourced key-issuing as well as decryption needs. The difficulties in establishing fine-grained access control over encrypted data in cloud computing are the most crucial information in this work. One-to-many encryption using public keys is made possible by a brand-new public key primitive called attribute-based encryption, which is presented to the cryptographic community.Although ABE offers a viable foundation for developing granular access control schemes in cloud computing, there are still a number of obstacles to overcome. One of the key issues with ABE is that when more attributes are given in the access policy, the computing cost for the decryption step increases. In addition, the creation of the user's private key in the present ABE schemes necessitates several modular exponentiations. The authority must update keys for the leftover users with his or her characteristics in order to revoke a single user from an existing ABE. The entire access control system's efficiency would be constrained by the authority end if all of these demanding responsibilities were centralised there [4].

This work introduces a technique called Ciphertext-Policy Attribute-Based Encryption for implementing complicated access control on encrypted data. It makes use of characteristics to define a user's credentials, and whomever encrypts the data sets the rules for who is permitted to decode it. By storing data locally on a trusted server and using system optimisations, traditional access control is implemented. The amount of time required to decrypt data while utilising the recursive DecryptNode technique and randomly selecting the nodes that satisfy each threshold gate is shown on the line labelled "naive". Running time is increased by merging pairs of leaf nodes with the same attribute because exponentiations in G0 are more costly than in G1.Before enabling a user to access records or files, the server is trusted as a reference monitor to verify that the user has the appropriate certification. To solve this problem, the Ciphertext-Policy Attribute Based Encryption system was developed. It allows for a novel type of encrypted access control in which the party encrypting the material can declare a policy over these characteristics stating a set of characteristics describes the users' private keys and the encryptions that they are permitted to decipher. The system is impervious to collusion attacks and allows policies to be specified as any monotonic tree access structure. Finally, a system implementation was offered, along with a number of optimisation methods [5].

3. PROPOSED SYSTEM

The suggested system included Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption. Unlike the method of independently encrypting a second random message subsequently committing to the real message by employing this random message, this CPA-secure design uses only one random message. In this procedure, a message and a random value are encrypted, and the message is then committed using the random value. The ciphertext size is reduced and the computational costs are lower with this general architecture. Additionally, it helps us more naturally acquire general RCCA-secure construction.

This technique may also be used to create selectively CPA-secure/RCCA-secure ABE systems with verifiable outsourced decryption in ABE systems that selectively employ CPA security with outsourced decryption. Considering that the

methods utilised to create our RCCA-secure transformation may be used to automatically create CCA-secure ABE from CPA-secure ABE, which we think to be of independent importance, is also significant. This is because A standard ABE scheme basically gets transformation processes added to it when it has outsourced decryption. CPA-secure ABE scheme with external decryption must include ciphertext verifiability or delegation capability as its foundation in this RCCA-secure architecture in order to respond to decryption requests. The following benefits of the suggested strategy are listed:

- It requires less calculation and has more condensed ciphertext.
- It is more versatile.
- It is more dependable.
- It is simple to get from our standardised RCCA-secure structure.

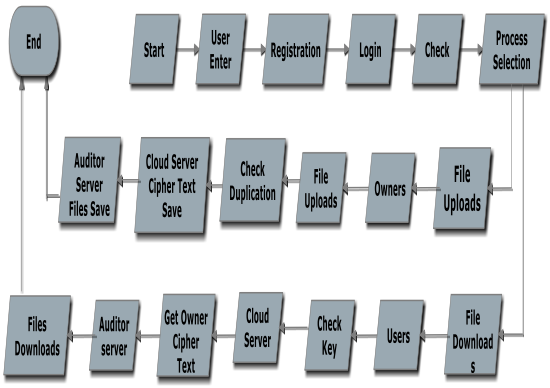

Fig 1: System Architecture

The next section provides an explanation of the many phases that are involved in putting the suggested technique into practise:

1. File Uploads(Encryption)

In this procedure, a message and a random value are encrypted, and the message is then committed using the random value. Our scheme is more general, requires less processing, and produces smaller ciphertext. Additionally, it helps us more naturally acquire general RCCA-secure construction.

2. Cloud Server

The decryption processes of ABE systems must be sped faster, especially on some devices with restricted resources. Users may delegate pairing calculations to a third party using the suggested pairing delegation procedures. However, the disadvantage that the computational cost is inversely correlated with the complexity of the access policy still persists when employing paired delegation strategies used in decryption procedures of the ABE system. There are a number of compromises made with regards to effectiveness as well as security to hasten the decryption of ABE systems.

3. Auditor Server

The approach used a message and a random value are both encrypted in our CPA-secure construction before the message is committed using the random value. This method entails separately encrypting an additional random message, which is then used to commit to the actual message. Our approach has a lot of advantages. First, our approach is more general, produces ciphertext that is more compact, and requires less processing. Second, it is more natural to convert including generic CPA-secure design into a general RCCA-secure construction.

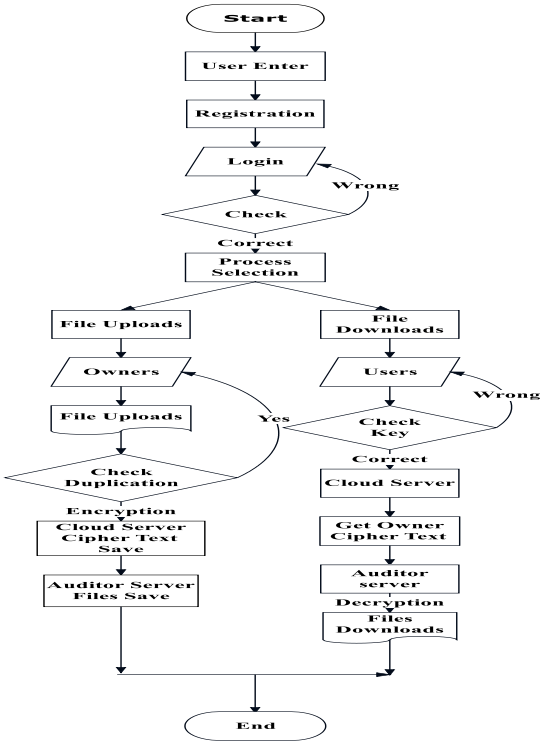

Fig 2: Flow Diagram

4. File Downloads (Decryption)

A novel approach model has been developed to significantly reduce the amount of the ciphertext as well as the decryption complexity for users in ABE platforms. In general, they encrypted an additional random message and added it to the ciphertext along with a checksum value that was calculated using this additional random message and the real plaintext. This checksum value is used to determine whether the transformation was carried out successfully and serves as a commitment to the true plaintext.

4. RESULTS

In this effort, we offer generic CPA- along with RCCA-secure ABE systems with verifiable external decryption. These systems are CPA-secure

ABE derivatives with external decryption. The system instantiates, the CPA-secure development in the standard model and starts with a CPA secure ABE scheme with outsourced decryption. The ciphertext size is reduced and the computational costs are lower with this general architecture. It may also be used to create selectively CPA-secure/RCCA-secure ABE systems with verifiable outsourced decryption in selectively CPA-secure ABE systems with outsourced decryption. By using the key blinding approach, the underlying CPA-secure ABE scheme with outsourced decryption is acquired. From this attribute-based KEM version, a symmetric session key is then generated, and all communications are encrypted using this session key.Furthermore, the generic RCCA-secure design may be used to quickly create an RCCA-secure ABE scheme in the standard model with verifiable outsourced decryption.

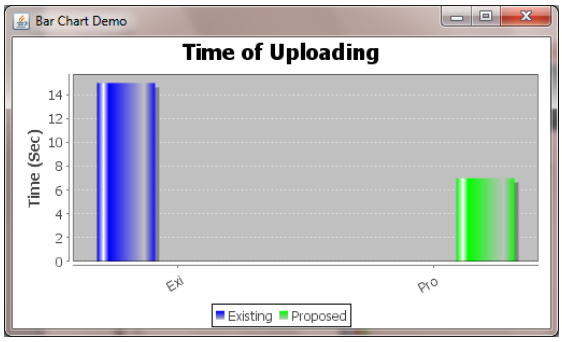

Fig 3: Comparative Analysis {Time of Uploading)

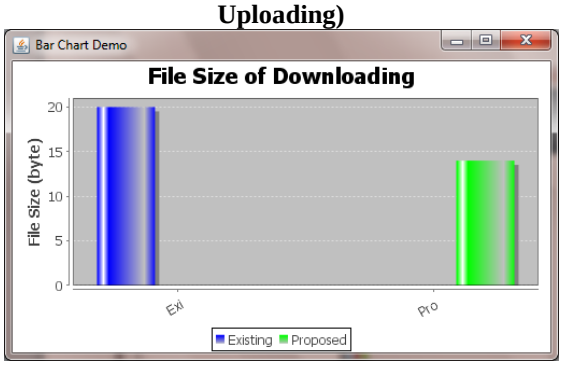

Fig 4: Comparative Analysis (Download)

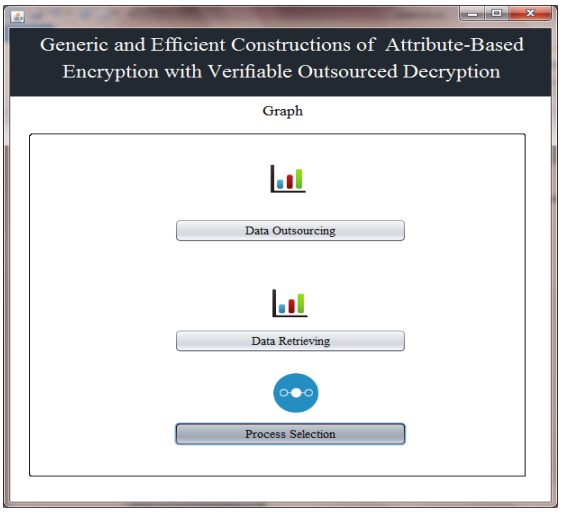

Fig 5: Performance Analysis

5. CONCLUSION

The system has suggested an Attribute-Based Encryption with Verifiable Outsourced Decryption construction for this project. Unlike the method of independently encrypting a second random message followed by committing to the real message through the utilisation of this random message, this CPA-secure design uses only one random message. In this procedure, a message and a random value are encrypted, and the message is then committed using the random value. The methods used in RCCA-secure construction may be used to create CCAsecure ABE from CPA-secure ABE in general.This concrete scheme's compliance with the accuracy criteria is very discernible. The CP-ABE system with outsourced decryption's underlying security is obtained by using the key blinding approach. The attribute-based KEM variation is then used to generate a symmetric session key, which is used to encrypt all communications using a symmetric encryption method. It's also crucial to note that our general RCCA-secure structure makes it simple to create a verified outsourced decryption ABE technique with RCCA security in the common architecture. Then, we put our CPA-secure instantiation into practise.

REFERENCE

[1] "Fuzzy identity based encryption", Florent LLOMBARD Lambert ROSIQUE, 2013.
[2] "Functional Encryption: Definitions and Challenges", Dan Boneh, Amit Sahai, 2011.
[3] "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Vipul Goyal, Omkant Pandey Amit Sahai Brent Waters, 2006.
[4] "Fine-Grained Access Control System based on Outsourced Attribute-based Encryption", Jin Li , Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma4, Wenjing Lou, 2013.

[5] "Ciphertext-Policy Attribute-Based Encryption", John Bethencourt, 2007.
[6] "Outsourcing the Decryption of ABE Ciphertexts", Matthew Green, Susan Hohenberger, 2011.
[7] "Toward Hierarchical Identity-Based Encryption", Jeremy Horwitz and Ben Lynn, 2002.
[8] "A Verifiable Cloud Storage using Attribute Based Encryption and Outsourced Decryption with Recoverability", R.V.Agalya, K.KarthikaLekshmi, 2010.
[9] "Attribute based encryption with verifiable outsourced description", Jun zuoLai , Robert H . Den g ,Chaowen Guan , and Jian Weng, 2013.
[10] "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization", Brent Waters, 2011.