https://dx.doi.org/10.24001/ijaems.3.4.9 *ISSN: 2454-1311*

A Novel Approach for Data Uploading and Remote Data Integrity Checking Based On Public Key Cryptography

K.Lakshmi Ragini[1], V.Rani Mounika[2], K.Sandeep[3]

Dept. of IT, Lakireddy Balireddy College of Engineering, Andhra Pradesh, India

Abstract— *As the technology is increasing more number of clients would like to store their data in the public cloud. As the cloud offer client to store large amount of data and can use the data from anywhere using the internet. New security problems need to be solved to give intact to the client data available in the cloud. Client has to feel that their outsourced data is in the protected way in the cloud. From the security problems we propose "A NOVEL APPROACH FOR DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING BASED ON PUBLIC KEY CRYPTOGRAPHY" (ANDURIC-PKC). We will give the formal definition, system model and security model. Then a concrete ANDURIC-PKC protocol is built by using Generic group model and certificate management is not required. This protocol is efficient and flexible, this may be provably secured by using Computational Diffie-Hellman problem. Based on the original client authorization, the proposed protocol can realize the data integrity checking.*

Keywords— Cloud computing, data integrity checking, generic group model, identity-based cryptography, public key cryptography.

I. INTRODUCTION

Along with the fast development of computing and communication technique, an excellent deal of information area unit generated. These huge information wants other robust computation resource and bigger cupboard space. Over the last year cloud computing satisfies the appliance necessities and grows terribly quickly. Primarily, it takes the information process as a service, like storage, computing, information security etc. By victimization the public cloud platform, the shopper's area unit mitigated of the burden for storage management, universal information access with independent geographical locations, etc. Thus, a lot of and a lot of clients would love to store and method their information by victimization the remote cloud ADP system. In public cloud computing, the shoppers store their huge data within the remote public cloud servers. Since the keep information is outside of the management of the shoppers, it entails the protection risks in terms of confidentiality, integrity and handiness of data and repair. Remote information integrity checking could be a primitive which can be wont to win over the cloud shoppers that their information are unbroken intact. In some special cases, the information owner is also restricted to get access to the general public cloud server, the information owner can delegate the task of information process and uploading to the third party, as an example the proxy. On the opposite aspect, the remote data integrity checking protocol be economical to make it appropriate for capacity-limited finish devices. Thus, based on generic group model and proxy public key cryptography, we'll study ANDURIC-PKC protocol.

II. RELATED WORK

There exist many alternative security issues within the cloud computing [1], [2]. This paper is predicated on the analysis results of proxy cryptography, generic cluster model and information integrity checking publicly cloud. In some cases, the cryptologic operation are delegated to the third party, as an example proxy. Thus, we've got to use the proxy cryptography. Proxy cryptography may be an important cryptography primitive. In 1996, Mambo et al. [3] planned the notion of the proxy cryptosystem. Once the linear pairings are brought into the identity-based cryptography, identity-based cryptography becomes economical and sensible. Since identity based mostly cryptography becomes additional economical as a result of it avoids of the certificate management, additional and additional consultants are apt to check identity-based proxy cryptography. In 2013, Yoon et al. planned AN ID-based proxy signature theme with message recovery [4]. Chen et al. planned a proxy signature theme and a threshold proxy signature theme from the Weil pairing [5]. By combining the proxy cryptography with secret

https://dx.doi.org/10.24001/ijaems.3.4.9 *ISSN: 2454-1311*

writing technique, some proxy re-encryption schemes are planned. Liu et al. formalize and construct the attribute-based proxy signature [6]. Guo et al. bestowed a non-interactive certified public accountant (chosen-plaintext attack)-secure proxy re-encryption theme that is immune to collusion attacks in formation re-encryption keys [7]. Several alternative concrete proxy re-encryption schemes and their applications are planned [8]–[10]. Publicly cloud, remote information integrity checking is a crucial security downside. Since the clients' large information is outside of their management, the clients' information could also be corrupted by the malicious cloud server notwithstanding advisedly or accidentally. So as to handle the novel security downside, some economical models are bestowed. In 2007, Ateniese et al. planned demonstrable information possession (PDP) paradigm [11]. In PDP model, the checker can check the remote data integrity without retrieving or downloading the whole data. PDP is a probabilistic proof of remote data integrity checking by sampling random set of blocks from the public cloud server, which drastically reduces I/O costs. The checker can perform the remote data integrity checking by maintaining small metadata. After that, some dynamic PDP model and protocols are designed [12]–[16]. Following Ateniese et al.'s pioneering work, many remote data integrity checking models and protocols have been proposed [17]–[19]. In 2008, proof of retrievability (POR) scheme was proposed by Shacham et al. [20]. POR is a stronger model which makes the checker not only check the remote data integrity but also retrieve the remote data. Many POR schemes have been proposed [21]–[26]. On some cases, the client may delegate the remote data integrity checking task to the third party. In cloud computing, the third party auditing is indispensable [27]–[30]. By using cloud storage, the clients can access the remote data with independent geographical locations. The end devices may be mobile and limited in computation and storage. Thus, efficient and secure ANDURIC-PKC protocol is more suitable for cloud clients equipped with mobile end devices. From the role of the remote data integrity checker, all the remote data integrity checking protocols are classified into two categories: private remote data integrity checking and public remote data integrity checking. In the response checking phase of private remote data integrity checking, some non-public data is indispensable. On the contrary, non-public data isn't needed within the response checking of public remote information integrity checking. Specially, once the non-public data is delegated to the third party, the third party may also perform the remote information integrity checking. During this case, it's conjointly referred to as delegated checking.

III. CONTRIBUTIONS

In public cloud, this paper focuses on the identity-based proxy-oriented knowledge uploading and knowledge integrity checking. By victimization identity-based public key scientific discipline, our proposed ANDRIC-PKC protocol is economical since the certificate management is eliminated. ANDRIC-PKC may be a novel proxy-oriented data uploading and remote knowledge integrity checking model in public cloud. We have a tendency to provide the formal system model and security model for ANDRIC-PKC protocol. Then, supported the generic cluster model, we have a tendency to designed the primary concrete ANDRIC-PKC protocol. Within the random oracle model, our designed ANDRIC-PKC protocol is demonstrably secure. Supported the initial client's authorization, our protocol will understand non-public checking, delegated checking and public checking.

IV. PAPER ORGANIZATION

The paper is organized below. The formal system model and security model of ANDRIC-PKC protocol are given in Section 4.1 the concrete protocol, performance analysis are presented in 6. Section 5 analyzes the proposed ANDRIC-PKC protocol's security. The proposed protocol is provably secure. At the end of the paper, the conclusion is given in Section 8.

4.1 SYSTEM MODEL AND SECURITY MODEL OF ANDRIC-PKC

In this section, we give the system model and security model of ANDRIC-PKC protocol. An ANDRIC-PKC protocol consists of four different entities which are described below:

1. OriginalClient: an entity, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.
2. PCS (Public Cloud Server): an entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients' data.
3. Proxy: an entity, which is authorized to process the OriginalClient's data and upload them, is selected and authorized by OriginalClient. When Proxy satisfies the warrant mω which is signed and issued by Original- Client, it can process and upload the original client's data; otherwise, it cannot perform the procedure.
4. KGC (Key Generation Center): an entity, when receiving an identity, it generates the private key which corresponds to the received identity.

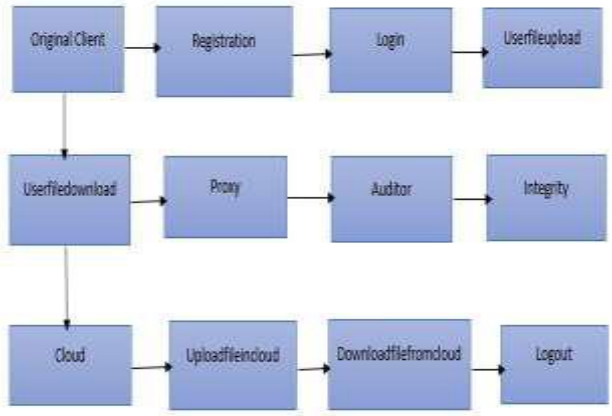
https://dx.doi.org/10.24001/ijaems.3.4.9 *ISSN: 2454-1311*

In our proposed ANDRIC-PKC protocol, OriginalClient will interact with PCS to check the remote data integrity. Thus, we give the definition of interactive proof system. Then,we give the formal definition and security model of ANDRIC-PKCprotocol.

4.2 SECURITY REQUIREMENTS

1. Original Client can perform the ID-PUIC protocol without the local copy of the file(s) to be checked.
2. Only if the proxy is authorized, i.e., it satisfies the warrant mω, the proxy can process the files and upload the block-tag pairs on behalf of Original Client.
3. Original Client cannot counterfeit the proxy to generate block-tag pairs, i.e., the proxy-protection property is satisfied.
4. If some challenged block-tag pairs are modified or lost, PCS's response cannot pass Original Client's integrity checking.

4.3 SYSTEM ARICTECHTURE:



1. In our architecture first client register and then client and proxy send their ID's to the private key generator.
2. Then PKG send the private keys Skid to the client and proxy.
3. By receiving private key proxy would like to access the data from the cloud.
4. While accessing the data from the PCS will interact with the original client whether proxy received warranty signature from the client.

Integrity is provided to the data by using the PKG (Private Key Generator). The Private Key Generator is dependable to create every clients private key by utilizing the related ID data (e.g. e-mail address, name or social security number). In this way, no certificate and PKI are required in the related cryptographic system under ANDRIC-PKC settings. ID based encryption (IBE) allows a sender to encrypt message straight forwardly by using a recipients ID without checking the approval of public key certificate. As need be, the recipient utilizes the private key respective with her/his ID to decrypt such cipher text. A public key setting needs to give client revocation approach, the earlier problem on the best way to revoke misbehaving/compromised users in an ANDRIC-PKC setting is actually raised.

V. PROPOSED WORK

Based on the original client's authorization, the protocol can realize private checking, delegated checking and public checking. The concrete ANDRIC-PKC protocol is provably secure and efficient by using the formal security proof and efficiency analysis. By using identity-based public key cryptology, the proposed ANDRIC-PKC protocol is efficient since the certificate management is eliminated. Then, based on the generic group model, we designed the first concrete ANDRIC-PKC protocol. In which it can answer the question: "What is the fastest generic algorithm for breaking a cryptographic hardness assumption". A generic algorithm is an algorithm that only makes use of the group operation, and does not consider the encoding of the group.

VI. PERFORMANCE EVALUATION

Performance analysis is a way to measure how far the product designed has met the requirements of the design as stated. To analyze the performance of our project built based on ANDRIC-PKC protocol is compared with two protocols namely Wang, Zhang and ID-PUIC. In this evaluation graph is plotted between taggen, public cloud server cost and the checker cost. These values are plotted in a graph as shown in the below figure.

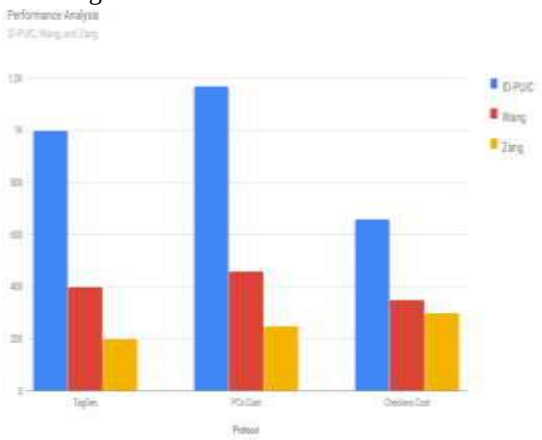


Fig : Performance Evaluation

When compared with this protocols our ANDRIC-PKC protocol is more flexible and can have less computations. And also the communication cost also reduced. This can be done by using the generic group model in our paper.

https://dx.doi.org/10.24001/ijaems.3.4.9 *ISSN: 2454-1311*

VII. CONLUSION

In this paper, this complimentary proposes the modern security work of ANDRIC-PKC in public cloud. The complimentary formalizes ANDRIC-PKC's system model and warranty model. Then, the first concrete ANDRIC-PKC protocol is designed by using the generic group model technique. The concrete ANDRIC-PKC guideline is provably secure and factual by using the formal security proof and simplicity analysis. On the other hand, the approaching ANDRIC-PKC protocol can also realize nonpublic remote data principle checking, delegated remote data fairness checking and public remote data principle checking based on the original client's authorization

REFERENCE

[1] Wang, Huaqun, Debiao He, and Shaohua Tang. "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud." *IEEE Transactions on Information Forensics and Security* 11.6 (2016): 1165-1176.

[2] Zhangjie, Fu, et al. "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing." *IEICE Transactions on Communications* 98.1 (2015): 190-200.

[3] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *J. Internet Technol.*, vol. 16, no. 2, pp. 317–323, 2015.

[4] Mambo, Masahiro, Keisuke Usuda, and Eiji Okamoto. "Proxy signatures for delegating signing operation." *Proceedings of the 3rd ACM conference on Computer and communications security*. ACM, 1996.

[5] Yoon, Eun-Jun, YongSoo Choi, and Cheonshik Kim. "New ID-based proxy signature scheme with message recovery." *International Conference on Grid and Pervasive Computing*. Springer Berlin Heidelberg, 2013.

[6] Chen, Bing-Chang, and Her-Tyan Yeh. "Secure proxy signature schemes from the Weil pairing." *The Journal of Supercomputing* 65.2 (2013): 496-506.

[7] Liu, Ximeng, et al. "Personal health records integrity verification using attribute based proxy signature in cloud computing." *International Conference on Internet and Distributed Computing Systems*. Springer Berlin Heidelberg, 2013.

[8] Guo, Hui, Zhenfeng Zhang, and Jiang Zhang. "Proxy re-encryption with unforgeable re-encryption keys." *International Conference on Cryptology and Network Security*. Springer International Publishing, 2014.

[9] Kirshanova, Elena. "Proxy re-encryption from lattices." *International Workshop on Public Key Cryptography*. Springer Berlin Heidelberg, 2014.

[10] Ateniese, Giuseppe, et al. "Provable data possession at untrusted stores." *Proceedings of the 14th ACM conference on Computer and communications security*. Acm, 2007.