ISSN 2395-1621

Intensify the Efficiency and Security for Multi User Data Sharing using Key Agreement protocol in cloud computing

[#1]Mr.Vivek JaysingNagargoje, [#2]Prof.Manisha Darak

[1]viv7799@gmail.com
[2]darakmanisha9@gmail.com

[#12]Department of Computer Engineering
Siddhant College of Engineering Sadumbare

ABSTRACT

Data sharing in cloud computing permits multiple participants to freely share the cluster knowledge that improves the efficiency of labour in cooperative environments and has widespread potential applications. However, a way to build positive the protection knowledge info} of information sharing among and therefore the because of efficiently share the out sourced information in Associate in Nursing terribly cluster manner unit of activity formidable challenges. Note that key agreement protocols have contend a awfully necessary role in secure and economical cluster knowledge sharing in cloud computing. throughout this paper, by taking advantage of the Centro parallel balanced incomplete block vogue (SBIBD), we've a bent to tend to gift a unique block design-based key agreement protocol that supports multiple participants, which can exile extend the number of participants in Associate in Nursing terribly cloud surroundings the structure of the block vogue. Supported the planned cluster knowledge sharing model, we've a bent to gift general formulas for generating the common conference key K for multiple participants. Note that by taking advantage of the block vogue, the tactic complexness of the planned protocol linearly can increase with the number of participants and also the communication quality is greatly reduced. To boot, the fault tolerance property of our protocol permits the cluster knowledge sharing in cloud computing to face to utterly completely different key attacks, that's analogous to protocol.

Keywords—Key agreement protocol, centro symmetric balanced incomplete block style (SBIBD), data sharing, cloud computing.

ARTICLE INFO

Article History

Received: 23rd July 2019

Received in revised form :

23rd July 2019

Accepted: 25th July 2019

Published online :

30th July 2019

I. INTRODUCTION

Cloud computing and cloud storage became hot topics in recent decades. unit dynamical the approach we've an inclination to measure and greatly rising production efficiency in some areas. At present, due to restricted storage resources and additionally the necessity for convenient access, we've an inclination to love higher to store all sorts of data in cloud servers, that's to boot AN honest chance for firms and organizations to avoid the overhead of deploying and maintaining instrumentality once data unit keep regionally. The cloud server provides degree open and convenient storage platform for folks and organizations, however it additionally introduces security problems. As AN example, a cloud system might even be subjected to attacks from every malicious users and cloud suppliers. In these eventualities, it is vital to confirm the protection of the keep data among the cloud. In several schemes were planned to preserve the privacy of the outsourced data. The upper than schemes only thought-about security problems with one data owner. However, in some applications, multiple data householders would adore to firmly share their data throughout a cluster manner. Therefore, a protocol that supports secure cluster data sharing beneath cloud computing is needed. A key agreement protocol is utilized to urge a regular conference key for multiple participants to create certain the protection of their later communications, and this protocol is applied in cloud computing to support secure and economical knowledge sharing. Since it completely was introduced by Diffie-Hellman in their seminal paper, the key agreement protocol has become one of the essential crypto logical primitives. the essential version of the Diffie-Hellman protocol provides degree economical answer to the matter of constructing a regular secret key between a pair of participants. In cryptography, a key agreement protocol might be a protocol among that a pair of or further parties will agree on a key in such the method that every influence the result. By mistreatment the key agreement protocol, the conferees will firmly send and receive messages from each

other mistreatment the common conference key that they agree upon beforehand. Specifically, a secure key agreement protocol ensures that the individual cannot get the generated key by implementing malicious attacks, like eavesdropping. Thus, the key agreement protocol is wide used in interactive communication environments with high security needs (e.g., remote board conferences, teleconferences, cooperative workspaces, oftenest identification cloud computing thus on). The Diffie-Hellman key agreement provides the thanks to generate keys. However, it does not offer degree authentication service, that creates it in danger of man within the middle attacks. this instance is addressed by adding some sorts of authentication mechanisms to the protocol, as planned by Law et al. in. to boot, the Diffie-Hellman key agreement can only support a pair of participants. afterwards, to resolve the varied key attacks

II. LITERATURE SURVEY

A. Main Contribution

In this project, we present an efficient and secure blockdesign-based key agreement protocol by extending the structure of the SBIBD to support multiple participants, which enables multiple data owners to freely share the outsourced data with high security and efficiency. Note that the SBIBD is constructed as the group data sharing model to support group data sharing in cloud computing. Moreover, the protocol can provide authentication services and a fault tolerance property. The main contributions of this paper are summarized.

B. Related Works

It is well known that data sharing in cloud computing can provide scalable and unlimited storage and computational resources to individuals and enterprises. However, cloud computing also leads to many security and privacy concerns, such as data integrity, confidentiality, reliability, fault tolerance and so on. Note that the key agreement protocol is one of the fundamental cryptographic primitives, which can provide secure communication among multiple participants in cloud environments.

C. Papers

Paper 1. Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data

With the arrival of cloud computing, information house owners square measure intended to source their complicated information management systems from native sites to the business public cloud for excellent flexibility and economic savings. except for protective information privacy, sensitive information should be encrypted before outsourcing, that obsoletes ancient information utilization supported plaintext keyword search. Thus, sanction native Associate in Nursing encrypted cloud information search service is of dominant importance. Considering the massive variety of knowledge users and documents within the cloud, it's necessary to permit multiple keywords within the search request and come documents within the order of their connectedness to those keywords. connected works on searchable encoding concentrate on single keyword search or mathematician keyword search, and barely type the search results. during this paper, for the primary time, we tend to outline and solve the difficult downside of privacy conserving multi-keyword hierarchal search over encrypted cloud information (MRSE). we tend to establish a collection of strict privacy needs for such a secure cloud information utilization system.

Paper 2. sanctionActive Cloud Storage Auditing with Key-Exposure Resistance

Cloud storage auditing is viewed as a very important service to verify the integrity of the info publicly cloud. Current auditing protocols square measure all supported the belief that the shoppers secret key for auditing is completely secure. However, such assumption might not invariably be control, because of the probably weak sense of security and/or low security settings at the shopper. If such a secret key for auditing is exposed, most of this auditing protocols would inevitably become unable to figure. during this paper, we tend to concentrate on this new facet of cloud storage auditing. we tend to investigate the way to cut back the harm of the shoppers key exposure in cloud storage auditing, and provides the primary sensible resolution for this new downside setting. we tend to formalize the definition and also the security model of auditing protocol with key-exposure resilience and propose such a protocol. In our style, we tend to use the binary tree structure and also the pre-order traversal technique to update the key keys for the shopper. we tend to additionally develop a unique critic construction to support the forward security and also the property of block less terribly ability. the safety proof and also the performance analysis show that our planned protocol is secure and economical.

Paper 3. Sanction active Cloud Storage Auditing With Verifiable Outsourcing of Key Updates

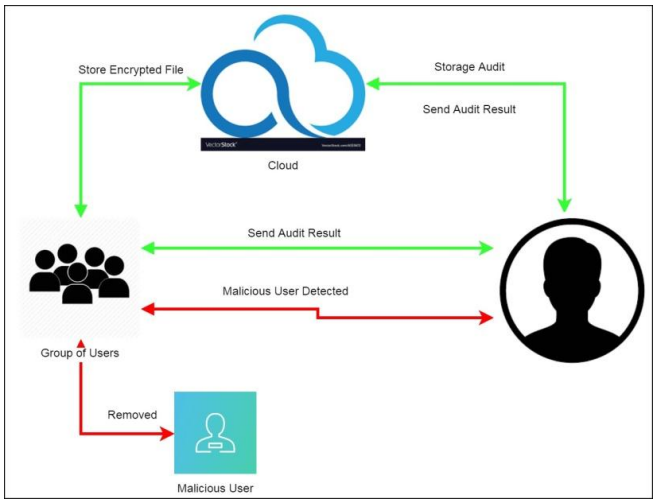
Key-exposure resistance has invariably been a very important issue for in-depth cyber defence in several security applications. Recently, the way to wear down the key exposure downside within the settings of cloud storage auditing has been planned and studied. to handle the challenge, existing solutions all need the shopper to update his secret keys in when amount, which can inevitably usher in new native burdens to the shopper, particularly those with restricted computation resources, like mobile phones. during this paper, we tend to concentrate on the way to create the key updates as clear as potential for the shopper and propose a brand new paradigm known as cloud storage auditing with verifiable outsourcing of key updates. during this paradigm, key updates are often safely outsourced to some licensed party, and so the key-update burden on the shopper are going to be unbroken bottom. specially, we tend to leverage the third party auditor (TPA) in several existing public auditing styles, let it play the role of licensed party in our case, and create it answerable of each the storage auditing and also the secure key updates for key-exposure resistance.

III. PROPOSED METHODOLOGY

The system model of our group data sharing scheme in cloud computing is illustrated in Fig. 1. A TPA, cloud and users are involved in the model, where the TPA is responsible for cloud storage auditing, fault detection and generating the system parameters. The cloud, who is a semi trusted party, provides users with data storage services and download services. Users can be individuals or staff in a company. To work together, they form a group, upload data to the cloud server and share the outsourced data with the group members. In practice, users can be mobile Android devices, mobile phones, laptops, nodes in underwater sensor networks and so forth.

Moreover, the group data sharing model is based on the SBIBD, where a trusted third party is not required. The construction of the SBIBD group data sharing model is described in detail in Section 4. With respect to this model, all the participants exchange messages from intended entities according to the structure of the SBIBD to determine a common conference key.

A. Architecture

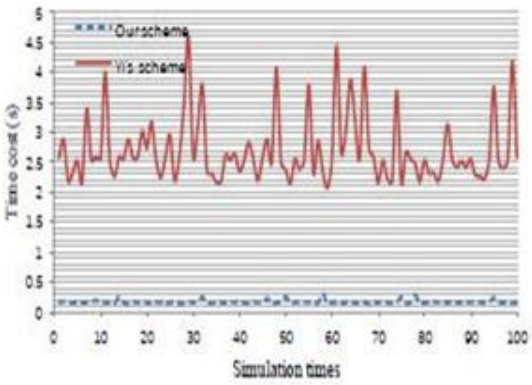


B. Algorithms

```
for i = 0; i < k; i + + do
        for j = 0; j <k; j + +
                do
        if j == 0 then
        Bi;j = 0;
        else
        Bi;j = ik + j;
        end if
        end for
end for
for i = k + 1; i < k2 + k; i + + do
        for j = 0; j < k; j + + do
                if j == 0 then
                Bi;j = b(i - 1) /kL;
        else
        Bi;j = jk+1+MODk(i-j+(j-1) b(i - 1)=kc);
        end if
        end for
end for
```

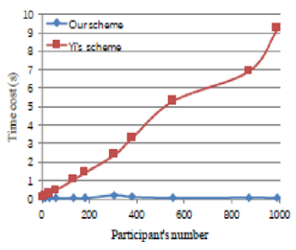
C. Mathematical Model

Input:
Large Bandwidth Network, movable device, sensor
Output:
Successful communication between two devices System Description
1. Input: Set of outsourced data sets by corresponding data user.
2. Output: Securely data sharing with group participant and remove malicious user from group through TPA.
3. System Used:
1. TPA for auditing on data and remove malicious users Let S is the system, S= I, P, O,IS,OS,F,G,f1,f2
Where,I-Input,
P- procedure,
O- Output.
I-F,G
F- data les set of f1,f2,,fn
G- Group Users Query g1,g2,,qN
Procedure(P):
Where :
TPA=Third Party Auditor,
F=FaultTolerance
B=Set of block.
V=No of group participant.
ei = PublicKey
di = PrivateKey
H1,h2=HashFunction
Identify failure cases as F
F=fshare data to malicious user in group.g
Identify success as s.
s=share data in group and give private key to all group participant and remove malicious user from group.

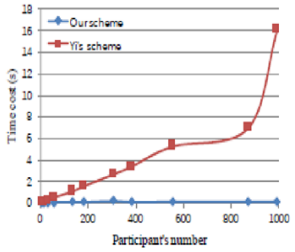


Efficiency comparison for different simulation times.

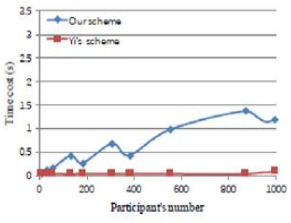
Efficiency comparison for different phases in Graphs



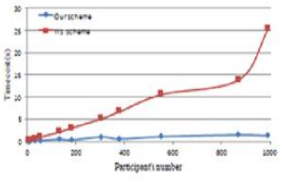
(a) Initial phase



(b) Key agreement phase



(c) Authentication phase



Efficiency comparison for multiple participants.

IV. RESULT AND DISCUSSIONS

A. *Adversary Model*

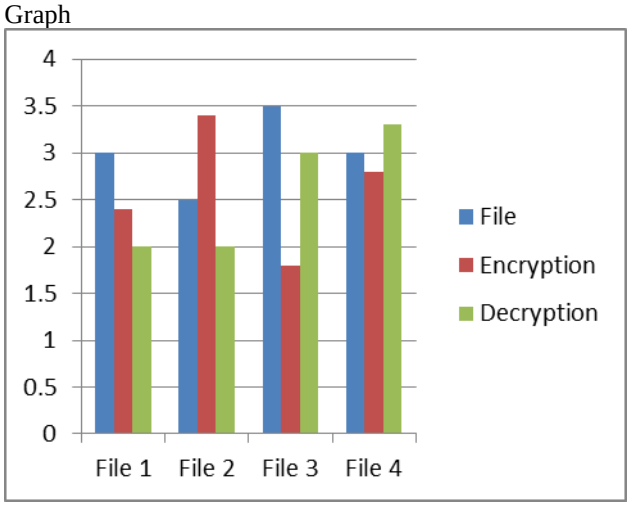
The adversary model determines the capabilities and possible
actions of the attacker. Similar to, the adversary model is defined as follows.

1. The adversary reveals a long-term secret key of a participant in a conference and then impersonates others to this participant.
2. The adversary reveals some previous session keys and then learns the information about the session key of a fresh participant. Consequently, the adversary can impersonate the fresh participant with the session key to others.
3. The adversary reveals the long-term keys of one or more participants in the current run. Then, the adversary attempts to learn the previous session key
4. A malicious participant chooses different sub keys, generates different signatures and broadcasts the messages to the corresponding participants, which makes the conference key derived by different participants distinct

B. *The Construction of Multi User Data Sharing Model*

To support a group data sharing scheme for multiple participants applying an SBIBD, we design an algorithm to construct the (v; k +1; 1)-design. Moreover, the constructed(v; k + 1; 1)-design requires some transformations to establish
the group data sharing model such that v participants can perform the key agreement protocol

FIGURES
Graph



[Graph 1:File Encryption and Decryption in ms(Time Unit)]

Here X axis indicates file number and y axis indicates time in msec.

File ID	File Size	Encryption	Decryption
File 1	3KB	2.4ms	2 ms
File 2	2.5KB	3.4 ms	2 ms
File 3	3.5KB	1.8 ms	3 ms
File 4	3KB	2.8 ms	3.3 ms

[Table No.1]

Table 1 shows that File1 having size 3KB is encryptedin 2.4ms and it gets decrypted in 2ms.File2 having size 2.5KB is encrypted in 3.4ms and it gets decrypted in 2ms.File3 having size 3.5KB is encrypted in 1.8ms and it gets decrypted in 3ms.File4 having size 2.8KB is encrypted in 2.8ms and it gets decrypted in 3.3ms.

V. CONCLUSIONS

As a development within the technology of the net and cryptography, cluster information sharing in cloud computing has opened up a replacement space of quality to pc networks. With the assistance of the conference key agreement protocol, the security and potency of cluster information sharing in cloud computing may be greatly improved. Specifically, the outsourced data of the information the info the information} house owners encrypted by the common conference key square measure shielded from the attacks of adversaries. Compared with conference key distribution, the conference key agreement has qualities of upper safety and responsible. However, the conference key agreement asks for an outsized amount of knowledge interaction within the system and additional computational price. To combat the issues within the conference key agreement, the SBIBD is used within the protocol design.
In this project, we tend to gift a completely unique block design-based key agreement protocol that supports cluster information sharing in cloud computing. because of the definition and therefore the mathematical descriptions of the structure of a (v; k + 1; 1)-design, multiple participants may be concerned within the protocol and general formulas of the common conference key for participant square measure derived. Moreover, the introduction of volunteers permits the given protocol to support thefault tolerance property, thereby creating the protocol additional practical and secure. In our future work, we might like to extend our protocol to produce additional properties (e.g.,anonymity, traceability, so on) to create it applicable for a variety of environments.

REFERENCES

[1] L. Zhou, V. Varadharajan, and M. Hitchens, “Cryptographic rolebased access control for secure Cloud data storage systems,” Information Forensics and ecurity IEEE Transactions on, vol. 10, no. 11, pp. 2381–2395, 2015
[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, “Secure cloud storage meets with secure network coding,” in IEEE INFOCOM, 2014, pp. 673–681.
[3] D. He, S. Zeadally, and L. Wu, “Certificateless public auditing scheme for cloud-assisted wireless body area networks,” IEEE Systems Journal, pp. 1–10, 2015.
[4] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[5] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, “An efficient rfid authentication protocol providing strong privacy and security,” Journal of Internet Technology, vol. 17, no. 3, p. 2, 2016
[6] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, “An efficient protocol for authenticated key agreement,” Designs Codes and Cryptography, vol. 28, no. 2, pp. 119–134, 2010.
[7] X. Yi, “Identity-based fault-tolerant conference key agreement,” IEEE Transactions on Dependable and

Secure Computing, vol. 1, no. 3, pp. 170–178, 2004.

[8] R. Barua, R. Dutta, and P. Sarkar, "Extending joux's protocol to multi party key agreement (extended abstract)." Lecture Notes in Computer Science, vol. 2003, pp. 205–217, 2003.

[9] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," Journal of Communications and Networks, vol. 14, no. 6, pp. 682–691,2012.

[10] B. Dan and M. Franklin, "Identity-based encryption from the weil pairing," Siam Journal on Computing, vol. 32, no. 3, pp. 213–229,2003.

[11] S. Blakewilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in IMA International Conference on Cryptography and Coding, 1997, pp. 30–45.

[12] I. Chung and Y. Bae, "The design of an efficient load balancing algorithm employing block design," Journal of Applied Mathematics and Computing, vol. 14, no. 1, pp. 343–351, 2004.

[13] O. Lee, S. Yoo, B. Park, and I. Chung, "The design and analysis of an efficient load balancing algorithm employing the symmetric balanced incomplete block design." Information Sciences, vol. 176, no. 15, pp. 2148–2160, 2006.

[14] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 79–88, 2011.

[15] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp.222–233, 2014.

