IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Review on Identity-Based Proxy Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud

Mangala L[1], Rajendra A B[2]

PG Scholar, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[1]

Professor& HOD, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[2]

Abstract: Impact of advanced technology has highly effected in our society. The economic view of world has completely changed with changes in technology. Cloud computing is the new range in wireless world. One of the major challenging issues is data integrity/security. This paper gives entire information to overcome these problems using various protocols.

Keywords: Cloud computing, identity based cryptography, proxy public key cryptography, remote data integrity checking.

I. INTRODUCTION

Cloud computing is a type of internet based computing that provides shared computer processing resources and data to computers and other devices on demand. Identity based cryptography is also known as public key cryptography publicly known string representing an individual or organisation is used as a public key.

Proxy public key cryptography allows third parties to alter a cipher text which has been encrypted for third party, so that it may be decrypted by another.

Remote data integrity checking is the crucial technology in cloud computing. The proposed protocol supports public verifiability without help of a third party auditors.

To overcome this problem, proposed a novel ID-PUIC protocol. ID-PUIC is based on system model and security model. Bilinear pairings designed the existing one and random oracle model gives protection to data leaking.

II. LITERATURE SURVEY

Y. Ren [1] Discussion of cloud storage is presently a hot research topic in data technology. In cloud storage, date security properties such as data classification, respectability and approachability becomes more and more profitable. Recently, many provable data possession (PDP) systems are proposed to secure data respectability. It needs to assign the remote information possession examining some proxy. These PDP system are not secure since the proxy stores some state data in distributed storage servers. To propose a proficient common verifiable provable data possession system, which uses Diffie-Hellman shared key to develop the homomorphic authenticator. Certainly, the verifier in our scheme is stateless and free of the cloud storage benefit. It is valid service, and is very productive compared with the previous PDP scheme, since the bilinear operation is not required.

E. Kirshanova [2] Inspired to obtain proxy re-encryption (PRE) was represented by Blaze, Bleumer and Strauss [Euro crypt '98]. Primarily, PRE allows a semi-trusted intermediary to change a cipher text encoded under single key into an encryption of the same plaintext under another key, without displaying the elementary plaintext. From exact point, absorbing appeals have been authenticated, and huge developments in distinct settings have been proposed. In 2007, Canetti and Honhenberger [CCS '07] featured a more grounded concepts – CCA-security and build a bi-directional PRE plot. Subsequently, a few work observed CCA secure PRE in view of bilinear gathering suppositions. Newly, Kirshanova [PKC] proposed the concept single-bounce CCA1-secure PRE conspire in light of learning with mistakes (LWE) supposition. In this task, First showed up an inconspicuous actual error in the security authentication of the work done by Kirshanova. This renew the aspect of grid based CCA1- secure developments, even in the free hop setting. At that point, Propose alternative LWE based single-bounce CCA1-secure PRE conspire. At long last, Huge development to bolster multi-bounce re-encryptions for different levels of security under various settings.

B. Chen, H. Yeh [3] An intermediary signature plan is a technique which permits a unique endorser to delegate his marking power to an assigned individual, called an intermediary underwriter. Up to now, the vast majority of intermediary mark plans depend on the discrete logarithm issue. In this paper, the propose an intermediary signature plot and an edge intermediary signature conspire from the Weil matching, furthermore give a security evidence.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Z. Fu [4] In recent years, consumer-centric cloud computing model has appeared as the growth of smart electronic devices merged with the visible cloud computing skills. A pattern of cloud services are convey to the client with the hypothesis that an powerful and successful cloud search solution is obtained. For clients, they desire to detect the related inputs, which is beneficial in cloud computing model. Sensitive data or information are encrypted before referencing to cloud, conventional keyword search techniques are unproductive.

Existing search commence over encrypted cloud information carries only accurate or frizzy keyword search, but not semantics multi-keyword ranked search. Hence, how to empower an beneficial searchable system with help of ranked search. It will remains a very difficult problem. In this article proposes an valid approach to resolve the problem of multi-keyword ranked search over encrypted cloud information supporting synonym queries. The main contribution of this article is encapsulated in two flavours : multi-keyword ranked search to execute more valid search results and synonym-based search to sustain synonym queries. More evaluation on real-world dataset were execute to prove the approach, showing that the proposed system solution is more powerful and beneficial for multi-keyword ranked searching in a cloud domain.

E. Yoon [5] Proposed an ID-based proxy signature scheme with message rehabilitation. To show that their agenda is helpless against the forgery attack, and an rival can produce a legitimate proxy signature for any message with past substantial proxy signature. Further, there is a security flaw in their proof. A article propose an enhanced scheme that rectify the deficiency of their scheme can be manifest the distinctive essential collection of message and ID attack accepting the computational Diffie-Hellman obstacles is hard.

Xi. Liu [6] In this novel, we have a inclination to proposed a theme known as attribute primarily based proxy signature. Then ABPS theme qualify a proxy signer to manifest the message on behalf of an native PHR owner. We have a tendency to tested our ABPS theme secure against existential. The forgery act against sort two or more person. Necessarily, we have a susceptibility to showed our ABPS theme acceptable for cloud computing environment to ensure the integrity of PHR.

S.Sree, Guhan [7] Delegation of checking is one of the essential security organizational approach to handle device verification in infinite network. Major problem deputes authentication utilises conventional proxy cryptography delegator controls the authority over messages, which are checked by delegator and in the proxy re-cryptography controlling the proxy from resigning unintended signature of delegate is not feasible. In order to solve, we propose beneficial delegation services called as conditional proxy re-signature. In this article, Proposed a security model for unidirectional conditional proxy re-signature, shows a concrete services and demonstrate the security of services in the random oracle model.

Xi.Yu Nai.cao [8] Proof of retrievability (POR) is a service programme to improve a validate storage on remote server that consumer can obtain the information, and Frequently accomplish an successful audit protocol to protect information is complete. In dynamics POR, the complication is to handle the latest variety of the information gains successful update and audit. In this article, proposed PDPOR that fulfil the best case O(log N) for update and audit protocols balanced with the best worse case rate and also the security of DPOR using simple methods.

Ganesh P Sachi N [9] An Intrusion detection system IDS supervises network transportation and system and describe to organiser. Instantly the intrusion detection also responds to malicious or harmful transportation taking action such as repulsing of user or authority from accessing the system. IDS has varieties of types but aims to notice corrupt system in various methods. There are two types of IDS such as network based and host based IDS. The IDS recognition for particular identification prospect of problems or hazards. The anomaly detection is used to differentiate trading against the inception. This discovery based on fuzzy and genetic algorithm, which intimate the process of natural evolution to identify its anatomy and framework.

R. Curt, Osama [10] Various storage networks depends on duplication to enlarge the accessibility and durability of information on suspicious storage network. Such storage network gives no confirmation or authentication to multiple copies of data are preserved. Storage server can conspire of data are that they preserve various copies of information, but they can store only one copy. To overcome this problem, proposed a multiple-replica provable data possession (MR-PDP). Provably server scheme that permits a consumer that preserves treplicas of file in storage system to authenticate through challenge response protocol. (1) Each specific replica can be build at a time. (2) Storage system uses t times the storage system involves to preserve a each replica. MR-PDP increases previous work on information possession proof for each copies of file in client/server storage system. Using MR-PDP to preserve t replica is additionally more successful than using one replica PDP schema to preserve t disparate or distinct files. Benefits of MRPDP can produce advance replica on insistence, Small expenditure when some of the replica is rejected.

III. PROPOSED SYSTEM

In public cloud, this article gives the clear explanation of Identity based proxy oriented data uploading and remote data integrity checking proficiency. In order to overcome the victimization, proposed a ID-PUIC protocol. ID-PUIC protocol is a novel proxy oriented data uploading and remote data integrity checking model in public cloud, intended to

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

formal and security model for ID-PUIC protocol. They supported linear pairing which designs the primary concrete ID-PUIC protocol. This ID-PUIC protocol is based on random oracle model. This is indisputable security, it supports the client approval. This protocol will notice delegate checking, private checking, public checking.

A. CONCRETE ID-PUIC PROTOCOL

This protocol based on 4 methods:

1. Original Client: User, which has enormous collection of data to be uploaded to public cloud server by proxy.
2. PCS (public cloud server): is an entity which handle valid storage capacity and computational resources to preserve the clients data.
3. Proxy: is an entity, which approves the task to original Client's information and upload them, This selection and consent by client.
4) KGC (Key Generation Centre): an entity, while obtaining accordance, it produces the private key, which parallel to the obtained accordance.

B. BILINEAR PAIRING

This ID-PUIC protocol on bilinear pairing. Signifying G1 and G2 as two cyclic multiplicative groups who have the same prime order q. Let $Z* q$ denote the multiplicative group of the field Fq. Bilinear pairings is a bilinear map.

$e : G1 \times G1 \rightarrow G2$

which satisfies the properties as shown below:

1) Bilinearity: $\forall$ g1, g2, g3 $\in$ G1 and a, b $\in$ $Z* q$,e(g1, g2g3) = e(g2g3, g1) = e(g2, g1)e(g3, g1)e(g1a, g2b) =e(g1, g2)ab
2) Non-degeneracy: $\exists$ g4, g5 $\in$ G1 such that e(g4, g5) 6=1G2 .
3) Computability: $\forall$ g6, g7 $\in$ G1,there is an efficient algorithm to compute e(g6, g7).

The concrete bilinear pairings e can be structured by using the Weil or Tate pairings on elliptic Curves. Our ID-PUIC protocol construction takes use of the of DDH (Decisional Diffie-Hellman) problem while its security is based on the hardness of CDH (Computational Diffie-Hellman) problem.

C. PERFORMANCE ANALYASIS

When adding time server to the system to determine individual file in instant time, and file is accessible to consumer or clients. When the time expire no file accessibility. So cloud are not suppose to store files for a long time.
Proxy server, While uploading files on cloud proxy stores copy of file so that if files on cloud are hacked by fraud or manipulation or integrity of files is not assure then, this files are restore from proxy.

IV. CONCLUSION

This paper proposes novel of ID-PUIC protocol, and design ID-PUIC's system model and security model. Then, initial concrete ID-PUIC protocol is meant by victimization the bilinear pairings technique. The concrete ID-PUIC protocol is indisputable security and economical by victimization the remote security proof and potential analysis.
ID-PUIC protocol also notice the private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking based on the original client's consent.

REFERENCES

[1] Y. Ren, J. Shen, J. Wang, J. Han, S. Lee, "Mutual verifiable provable data auditing in public cloud storage," Journal of Internet Technology, vol.16, no.2, pp.317-323, 2015.
[2] E. Kirshanova, "Proxy re-encryption from lattices", PKC 2014, LNCS 8383, pp. 77-94, 2014.
[3] B. Chen, H. Yeh, "Secure proxy signature schemes from the weil pairing", Journal of Supercomputing, vol. 65, no. 2, pp. 496-506, 2013.
[4] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Transactions on Communications, vol. E98-B, no. 1pp.190-200,2015.
[5] E. Yoon, Y. Choi, C. Kim, "New ID-based proxy signature scheme with message recovery", Grid and Pervasive Computing, LNCS 7861, pp.945-951, 2013.
[6] X. Liu, J. Ma, J. Xiong, T. Zhang, Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing", Internet and Distributed Computing Systems, LNCS 8223,pp. 238-251, 2013.
[7] S. Sree vivek, Guhan,"Controlled proxy re-signing-conditional proxy re-signatures "International joint conference one-Business and Telecommunication (ICETE), vol. 4, 2015.
[8] Xiaoqi Yu, Nairen Cao, Jun Zhamg , Siu-Ming Yiu, "Dynamic Proof of Retrievability with improved worst case over headed", IEEE Conference on Communication and Network Security, no.pp: 10.1109/CNS.2016.7860551, 2016.
[9] Ganesh Prasad Rout, Sachi Nandan Mohanty. "A Hybrid Approach for Network Intrusion Detection", Communication System and Network Technologies (CSNT), 2015.
[10] Reza Curtmola, Osama Khan, Randal Burns, Giuseppe Ateniese," MR-PDP Multiple-Replica Provable Data Possession", International Conference on Distributed Computing System, no.pp: 10.1109/ICDCS.2008.68,2008.