ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Proxy Oriented Data Uploading and Integrity Checking in Cloud Computing

Rakshitha Gatti G.S [1], Chandan Raj [2]

P.G. Student, Department of Computer science & Engineering, EWIT Engineering College, Bengluru, India[1]

Associate Professor, Department of Computer Science & Engineering, EWIT Engineering College, Bengluru, India[2]

ABSTRACT: Cloud computing is progressively popular. An outsized range of information square measure outsourced to the cloud by data homeowners actuated to access the large-scale computing resources and cost savings. In this paper, for the primary issues, new security problems have to be solved in order to help more clients process their data in public cloud. When the client is restricted to access PCS, he will delegate its proxy to process his data and upload them. As uploading files on cloud proxy stores copies of file so that if files on cloud are hacked or corrupted or integrity of files is not ensured then those files are again regenerate from proxy. On the other hand, remote data integrity checking is also an important security problem in public cloud storage. It makes the clients check whether their outsourced data is kept intact without downloading the whole data. From the security problems, we propose a novel proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography: IDPUIC (identity-based proxy-oriented data uploading and remote data integrity checking in public cloud). With the emergence of pervasive 64 bit computing we observe that it is more cost effective to compute a SHA512 than it is to compute a SHA-256 over a given size of data.

KEYWORDS: Cloud computing, Identity- based, Proxy public key, Remote data integrity checking, hash algorithm SHA 512/256.

I. INTRODUCTION

Cloud storage offers associate on-demand knowledge outsourcing service model, and is gaining quality owing to its snap and low maintenance value. However, this new knowledge storage paradigm in cloud brings regarding several difficult style problems that have profound influence on the protection and performance of the general system, since this knowledge storage is outsourced to cloud storage suppliers and cloud shoppers lose their controls on the outsourced knowledge. Remote knowledge integrity checking may be a primitive which may be accustomed win over the cloud shoppers that their knowledge area unit unbroken intact. In some special cases, the information owner is also restricted to access the general public cloud server the information owner can delegate the task of knowledge process and uploading to the third party, for instance the proxy. Cloud storage offers associate degree on-demand information outsourcing service model, and is gaining quality as a result of its physical property and low maintenance value. Identity -based public key system (ID-PKS) is an attractive alternative for public key cryptography. ID-PKS setting eliminates the demands of public key infrastructure (PKI) and certificate organization in customary public key settings. An ID-PKS setting comprises of clients and a trusted third party (i.e. private key generator, PKG). The PKG 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 ID-PKS 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 IDPKS setting is actually raised. The conventional public key setting to certificate revocation list (CRL) is a well-known revocation approach.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

CRL approach, if a party gets a public key and its related authentication, first approves them and then looks upward the CRL to guarantee that the public key has not been revoked. In this procedure requires the online help under PKI so that it will incur communication bottleneck.

Along with the rapid development of computing and communication technique, great deals of data are generated. These massive data needs more strong computation resource and greater storage space. Over the last years, cloud computing satisfies the application requirements and grows very quickly.
Essentially, it takes the data processing as a service, such as storage, computing, data security, etc.

II. RELATED WORK

In this section we are going to discussed related work of previously existed systems. Y. Ren et.al [1] Discussed to cloud storage is presently a hot research topic in data technology. In cloud storage, date security properties such as information classification, respectability and accessibility turn out to be increasingly critical in numerous business applications. Recently, many provable data possession (PDP) plans are proposed to secure information respectability. It needs to appoint the remote information possession checking undertaking to some proxy. These PDP schemes are not secure since the proxy stores some state data in distributed storage servers. To propose a proficient common verifiable provable data possession scheme, which uses Differ-Hellman shared key to develop the homomorphism authenticator. Specifically, the verifier in our scheme is stateless and free of the cloud storage benefit. It is significant that the introduced scheme is very productive compared with the previous PDP scheme, since the bilinear operation is not required.

E. Yoon et.al [3] .The proposed an ID-based proxy signature scheme with message recuperation. To show that their plan is helpless against the forgery attack, and an adversary can produce a legitimate proxy signature for any message with knowing a past substantial proxy signature. What's more, there is a security defect in their confirmation. A propose an enhanced scheme that cures the shortcoming of their scheme and the enhanced scheme can be demonstrated existentially unforgeable-adaptively picked message and ID attack accepting the computational Diffie-Hellman issue is hard.

Harendra Singh, Girraj Kumar Verma[4].In this paper, we've planned Associate in Nursing ID based proxy signature theme with message recovery. This theme desires smaller information measure in distinction to previous ID-based proxy signature schemes. Thus this theme is often a decent various for certificate primarily based proxy signatures used for mobile agent. The theme has been proven DS-EUF-ACMIA underneath the belief of hardness of the CDHP in random oracle model. The potency comparison, conjointly given for showing quality of proposal. Although, theme has designed for a message of fastened length, none the less it provides Associate in Nursing innovation regarding proxy signatures for low information measure. This theme is often extended to a message of capricious length, mistreatment partial message recovery.

Peng Xu , Hongwu Chen , Deqing Zou , Hai Jin[4]
Description: This paper planned a replacement PRE system. It permits proxy to remodel the IBE cipher texts of information homeowners to new cipher texts. And these new cipher texts will be decrypted by the correlative Elgamal personal keys of information shoppers. Therefore knowledge shoppers will share knowledge owners' cloud knowledge, albeit they're within the completely different cloud systems. Moreover, the planned PRE system doesn't want knowledge shoppers to register within the same cloud system with knowledge owner.
Giuseppe Ateniese, Randal Burns ,Reza Curtmola[5]
Description: We introduced a model for obvious information possession, within which it's fascinating to reduce the file block accesses, the computation on the server, and also the client-server communication. Our solutions for PDP match this model: They incur a coffee (or even constant) overhead at the server and need a tiny low, constant quantity of com medication per challenge. Key parts of our schemes area unit the homomorphism verifiable tags. They permit to verify information possession while not having access to the particular file. Experiments show that our schemes, which supply a probabilistic possession guarantee by sampling the server's storage, create it sensible to verify possession of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

enormous information sets. Previous schemes that don't enable sampling aren't sensible once PDP is employed to prove possession of enormous amounts of knowledge.

III. SYSTEM ARCHITECURE AND MODEL

3.1. ID-PUIC PROTOCOL MODEL

In public cloud, the point concentrates on the personality based intermediary arranged information transferring and remote information uprightness checking. By utilizing character based open key cryptology, our proposed ID-PUIC convention is proficient since the authentication administration is wiped out. ID-PUIC is a novel intermediary situated information transferring and remote information honesty checking model out in the open cloud. We give the formal framework model and security display for ID-PUIC convention. At that point, in view of the bilinear pairings, we planned the main solid ID-PUIC convention. In the irregular prophet show, our outlined IDPUIC convention is provably secure. In view of the first customer's approval, our convention can understand private checking, designated checking and open checking.

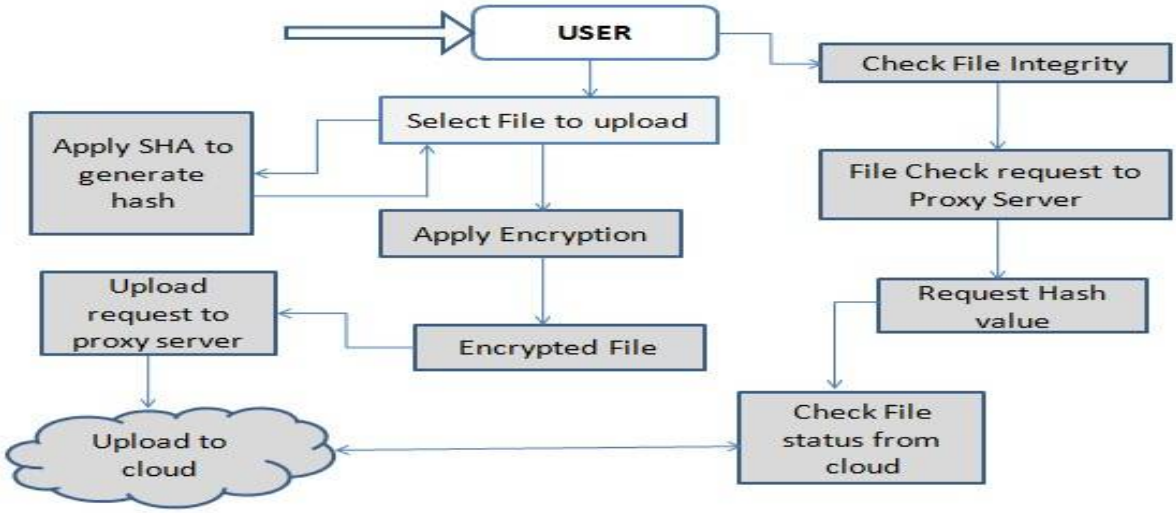

Figure 1: System Architecture

This solid ID-PUIC convention contains four strategies: Setup, Extract, Proxy-key era, TagGen, and Proof. In request to demonstrate the instinct of our development, the solid convention's design is portrayed in Figure 1.

An ID-PUIC convention comprises of four diverse substances which are depicted underneath**:**

1) Original Client: a substance, which has gigantic information to be transferred to PCS by the designated intermediary, can perform the remote information trustworthiness checking.

2) PCS (Public Cloud Server): a substance, which is overseen by cloud specialist co-op, has huge storage room what's more, calculation asset to keep up the customers' information.

3) Proxy: a substance, which is approved to prepare the Original Client's information and transfer them, is chosen and approved by Original Client. At the point when Proxy fulfills the warrant m! Which is marked and issued by Original-Customer, it can handle and transfer the first customer's information; else, it cannot play out the technique.

4) KGC (Key Generation Center): an element, while getting a character, it creates the private key which relates to the got character.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

3.2. Hash SHA 256/512

The performance of SHA-256 and SHA-512 depends on the length of the hashed message. Here we provide a summary. Generally, SHA-256 and SHA-512 can be viewed as a single invocation of an _init() function (that initializes the eight 64bit variable h0, h1, h2, h3, h4, h5, h6, h7), followed by a sequence of invocations of an _update() function, and an invocation a _finalize() function. The _finalize() function itself consists of one or two invocations of _update(), depending on the message's length. In addition, there are some operations to create a formatted "last block(s)" (also called "padding"). The _update() functions for SHA-256 and SHA-512 are different and, even more importantly, operate on different block sizes: 64 bytes for SHA-256 and 128 bytes for SHA-512. From a performance standpoint the contribution of the _init() function and the last block padding are negligible. Therefore, the performance of SHA-256 and SHA-512 can be quite accurately approximated from the performance of their respective _update() functions, and the number of invocations. The number invocations of the _update() function depends on the message length as follows.
SHA-256: Let M be a message of x bytes, $x = 64n + r$, $0 \leq m < 64$.
If $r \leq 55$, the number of calls to _update() is (n+1) If $r > 55$, the number of calls to _update() is (n+2)
Denote n = floor (x/64), r = x mod 64, and the cost (in CPU cycles) of one SHA-256 _update() function by UPDATE256.
The number of cycles for computing the SHA-256 of M is approximated by

UPDATE256 · (n + 1 + floor (r/55)) (1)

SHA-512: Let M be a message of y bytes, $y = 128m + s$, $0 \leq s < 128$. If $s \leq 111$, the number of calls to _update() is (m+1) If $s > 111$, the number of calls to _update() is (m+2)
Denote m = floor (x/64), s = y mod 64, and the cost (in CPU cycles) of one SHA-512 _update() function by UPDATE512.
The number of cycles for computing the SHA-512 of M is approximated by

UPDATE512 (m + 1 + floor (s/111)) (2)

IV. IMPLEMENTATION

Proxy server as Raspberry pi:

1 Raspberry pi having,2 Ethernet ports and a Wi-Fi adapter. Instead of uploading all the temperature data to the cloud and the cloud performing the time series prediction, in our implementation, the arduino boards tag the temperature data packets , on receiving the temperature data packets the raspberry pi (The Fog Network device) stores the temperature data and does a time series prediction on the data, the predicted data is then sent to the cloud , so that the cloud can display it on a webpage .

[6]The Raspberry Pi used in our implementation has 2 Ethernet ports and a Wi-Fi hotspot. The mother boards connect to the Wi-Fi of the Raspberry, they then measure the temperature of the surroundings every 5 seconds and send it to the router (the raspberry), on receiving the temperature data the raspberry invokes a python script that writes the received temperature values in different files (one file per mother board).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

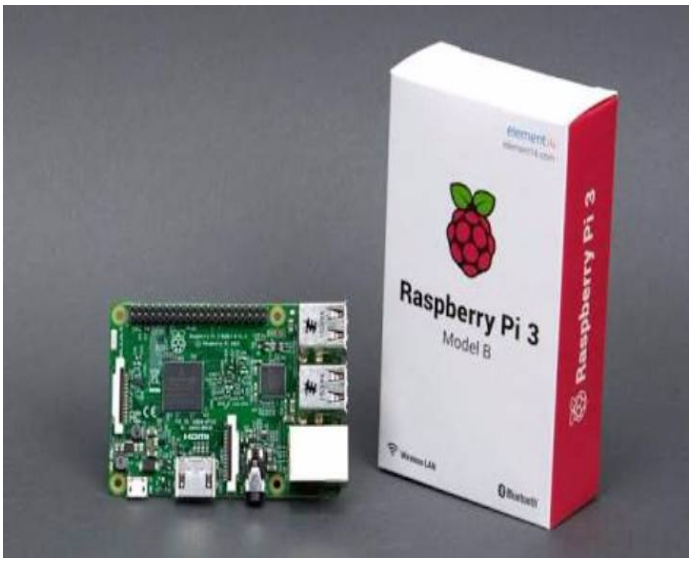

Figure 2.Raspberry Pi based proxy server.

The time series prediction is applied to the data in each file, the result of the time series prediction is then written into a mysql database instance running on the AWS cloud, the PHP instance on the cloud reads the values from mysql and displays it on a webpage. For a internet bandwidth of 1Mbps.

V. CONCLUSION

Roused by the application needs, this paper proposes the novel security idea of ID-PUIC in broad daylight cloud. The paper formalizes ID-PUIC's framework model and security display. At that point, the primary solid ID-PUIC convention is outlined by utilizing the HASH SHA-512 method. The solid ID-PUIC convention is provably secure and productive by utilizing the formal security verification and effectiveness examination. Then again, the proposed ID-PUIC convention can likewise acknowledge private remote information honesty checking, appointed remote information uprightness checking and open remote information honesty checking in light of the first customer's approval.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations further more thank the East west institute powers for giving the obliged base and backing. And we thank all the faculties for their support.

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] M. Mambo, K. Usuda, E. Okamoto, “Proxy signature for delegating signing operation”, CCS 1996,pp.48C57,1996.
[3] 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.
[4] Harendra Singh, Girraj Kumar Verma “ Message recovery” .
[5] B. Chen, H. Yeh, “Secure proxy signature schemes from the weil pairing”, Journal of Supercomputing, vol. 65, no. 2, pp. 496-506, 2013.
[6] Fung Po Tso, David R. White, Simon Jouet, Jeremy Singer, Dimitrios P. Pezaros The Glasgow Raspberry Pi Cloud:A Scale Model for Cloud Computing Infrastructures.
[7] 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

[8] H. Guo, Z. Zhang, J. Zhang, "Proxy re-encryption with unforgeable reencryption keys", Cryptology and Network Security, LNCS 8813, pp.20-33,2014.
[9] E. Kirshanova, "Proxy re-encryption from lattices", PKC 2014, LNCS 8383, pp. 77-94, 2014.
[10] P. Xu, H. Chen, D. Zou, H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage", Chinese Science Bulletin, vol.59,no.32, pp. 4201-4209, 2014.
[11] H. Wang, Q. Wu, B. Qin, J. Domingo-Ferrer, "FRR: Fair remote retrieval of outsourced private medical records in electronic health networks", Journal of Biomedical Informatics, vol. 50, pp. 226-233, 2014.
[12] H. Wang, "Anonymous multi-receiver remote data retrieval for pay-tv in public clouds", IET Information Security, vol. 9, no. 2, pp. 108-118, 2015.
[13] H. Shacham, B. Waters, "Compact proofs of retrievability", ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.
[14] Q. Zheng, S. Xu, "Fair and dynamic proofs of retrievability", CODASPY' 11, pp. 237-248, 2011.
[15] D. Cash, A. K¨upc¸ ¨u, D. Wichs, "Dynamic proofs of retrievability via oblivious ram", EUROCRYPT 2013, LNCS 7881, pp. 279-295, 2013.
[16] Ankit Lodha, Clinical Analytics – Transforming Clinical Development through Big Data, Vol-2, Issue-10, 2016.
[17] Ankit Lodha, Agile: Open Innovation to Revolutionize Pharmaceutical Strategy, Vol-2, Issue-12, 2016.