IDENTITY-BASED PROXY-ADAPTED DATA TRANSMISSION AND REMOTE DATA PRINCIPLEREVIEW IN CLOUD

Janagam Vamshi Krishna [1], Prof. N. Chandra Mouli[2]

1. **M.Tech Scholar, Department of CSE, Vaageswari College of Engineering, Karimnagar, Telangana, India– vamshikrishna.janagam@gmail.com, 9849173588**
2. **Associate Professor, Department of CSE , Vaageswari College of Engineering, Karimnagar, Telangana, India-cmnarsingoju@gmail.com, 9849750204**

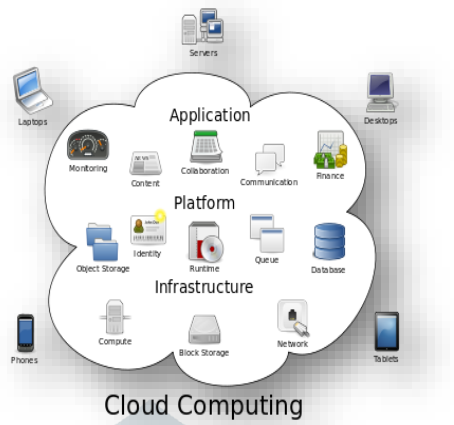
ABSTRACT:

More and more clients would like to store theirdata to public cloud servers (PCSs) along with the rapiddevelopment of cloud computing. New security problems haveto be solved in order to help more clients process their datain public cloud. When the client is restricted to access PCS, he will delegate its proxy to process his data and uploadthem. On the other hand, remote data integrity checking isalso an important security problem in public cloud storage.It makes the clients check whether their outsourced data are keptintact without downloading the whole data. From the securityproblems, we propose a novel proxy-oriented data uploading andremote data integrity checking model in identity-based publickey cryptography: identity-based proxy-oriented data uploadingand remote data integrity checking in public cloud (ID-PUIC).We give the formal definition, system model, and security model.Then, a concrete ID-PUIC protocol is designed using the bilinearpairings. The proposed ID-PUIC protocol is provably securebased on the hardness of computational Diffie–Hellman problem.Our ID-PUIC protocol is also efficient and flexible. Based on theoriginal client's authorization, the proposed ID-PUIC protocolcan realize private remote data integrity checking, delegatedremote data integrity checking, and public remote data integritychecking.

I.INTRODUCTION:

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computercannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is

unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Diagram clearly explain the about the secure computing

Working conditions and basic needs in the secure computing:

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

1. **Physical security:**

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.

Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

2. **Access passwords:**

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

3. **Prying eye protection:**

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

4. **Anti-virus software:**

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

5. Firewalls:

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

6. Software updates:

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.

Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

7. Keep secure backups:

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

8. Report problems:

If you believe that your computer or any data on it has been compromised, your should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

II.SYSTEM ARCHITECTURE

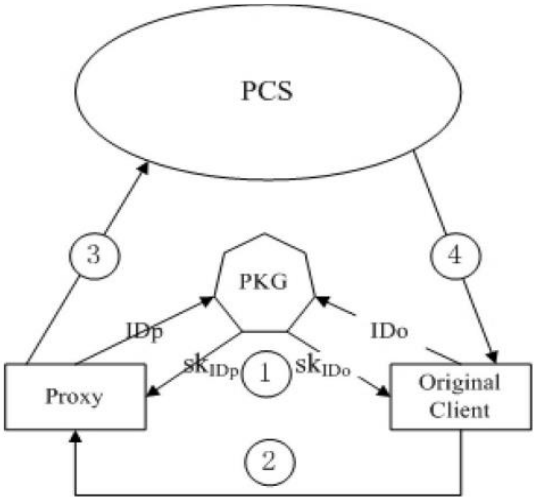


Fig. 1. Architecture of our ID-DPDP protocol.

III.EXISTING SYSTEM:

In public cloud environment, most clients upload their data to Public Cloud Server (PCS)and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion. But, the manager's legal business will go on during the period of investigation. When a large of data is generated,

who can help him process these data? If these data cannot be processed just in time, the manager will face the loss of economic interest. In order to prevent the case happening, the manager has to delegate the proxy to process its data, for example, his secretary. But, the manager will not hope others have the ability to perform the remote data integrity checking. Public checking will incur some danger of leaking the privacy. For example, the stored data volume can be detected by the malicious verifiers. When the uploaded data volume is confidential, private remote data integrity checking is necessary. Although the secretary has the ability to process and upload the data for the manager, he still cannot check the manager's remote data integrity unless he is delegated by the manager. We call the secretary as the proxy of the manager. In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity.

Disadvantages of Existing System:

1. In PKI, the considerable overheads come from the heavy certificate verification, certificates generation, delivery, revocation, renewals, *etc*.
2. In public cloud computing, the end devices may have low computation capacity, such as mobile phone, ipad, *etc*.

IV.PROPOSED SYSTEM:

In public cloud, this paper focuses on the identity-based proxy-oriented data uploading and remote data integrity checking. By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. ID-PUIC is a novel proxy-oriented data uploading and remote data integrity checking model in public cloud. We give the formal system model and security model for ID-PUIC protocol. Then, based on the bilinear pairings, we designed the first concrete ID-PUIC protocol. In the random oracle model, our designed ID-PUIC protocol is provably secure. Based on the original client's authorization, our protocol can realize private checking, delegated checking and public checking.

Advantages of Proposed System:

1. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis

V.IMPLEMENTATION:

MODULES:

- Original Client
- Public Cloud Server
- Proxy
- KGC

MODULE DESCRIPTIONS:

ORIGINAL CLIENT:

Original Client is an Entity, Who is going to act as an upload the massive data into the public cloud server (PCS) by the delegated proxy, and the main purpose is integrity checking of massive data will be through the remote control. For the Data uploading and Downloading client have to follow the following Process steps:

- Client can view the cloud files and also make the downloading.
- Client has to upload the file with some requested attributes with encryption key.
- Then client has to make the request to the TPA and PROXY to accept the download request and request for the secret key which will be given by the TPA.After receiving the secret key client can make the downloading file.

PUBLIC CLOUD SERVER:

PCS is an entity which is maintained by the cloud service provider. PCS is the significant cloud storage space and computation resource to maintain the client's massive data.

PCS can view the all the client's details and upload some file which is useful for the client and make the storage for the client uploaded files.

PROXY

Proxy is an entity, which is authorized to process the *Original Client*'s data and upload them, is selected and authorized by *Original Client*. When *Proxy* satisfies the warrant $m\omega$ which is signed and issued by *Original Client*, it can process and upload the original client's data; otherwise, it cannot perform the procedure.

Simply say means: without the Knowledge of Proxy's authentication and verification and acceptance of proxy client cannot download the file which is uploaded by the Client.

KGC

kgc (key generation center):an entity, when receiving an identity, it generates the private key which corresponds to the received identity.

generated secret key is send to the client who is make the request for the secret key via mail id which is given by the client.

VI.CONCLUSION:

Motivated by the application needs, this paper proposes the novel security concept of ID-PUIC in public cloud. The paper formalizes ID-PUIC's system model and security model. Then, the first concrete ID-PUIC protocol is designed by using the bilinear pairings technique. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis. On the other hand, the proposed ID-PUIC protocol can also realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking based on the original client's authorization.

VII.REFERENCES:

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Trans. Commun.*, vol. E98-B, no. 1, pp. 190–200, 2015.

[2] 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.

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in *Proc. CCS*, 1996, pp. 48–57.

[4] E.-J. Yoon, Y. Choi, and C. Kim, "New ID-based proxy signature scheme with message recovery," in *Grid and Pervasive Computing* (Lecture Notes in Computer Science), vol. 7861. Berlin, Germany: Springer- Verlag, 2013, pp. 945–951.

[5] B.-C. Chen and H.-T. Yeh, "Secure proxy signature schemes from the weil pairing," *J. Supercomput.*, vol. 65, no. 2, pp. 496–506, 2013.

[6] X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing," in *Internet and Distributed Computing Systems* (Lecture Notes in Computer Science), vol. 8223. Berlin, Germany: Springer-Verlag, 2013, pp. 238–251.

[7] H. Guo, Z. Zhang, and J. Zhang, "Proxy re-encryption with unforgeable re-encryption keys," in *Cryptology and Network Security* (Lecture Notes in Computer Science), vol. 8813. Berlin, Germany: Springer-Verlag, 2014, pp. 20–33.

[8] E. Kirshanova, "Proxy re-encryption from lattices," in *Public-Key Cryptography* (Lecture Notes in Computer Science), vol. 8383. Berlin, Germany: Springer-Verlag, 2014, pp. 77–94.
[9] P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," *Chin. Sci. Bull.*, vol. 59, no. 32, pp. 4201–4209, 2014.
[10] S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura, "Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption," in *Proc. CT-RSA Conf.*, vol. 9048. 2015, pp. 410–428.
[11] G. Ateniese *et al.*, "Provable data possession at untrusted stores," in *Proc. CCS*, 2007, pp. 598–609.
[12] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proc. SecureComm*, 2008, Art. ID 9.
[13] C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. CCS*, 2009, pp. 213–222.
[14] E. Esiner, A. Küpçü, and Ö. Özkasap, "Analysis and optimization on FlexDPDP: A practical solution for dynamic provable data possession," *Intelligent Cloud Computing* (Lecture Notes in Computer Science), vol. 8993. Berlin, Germany: Springer-Verlag, 2014, pp. 65–83.

[15] E. Zhou and Z. Li, "An improved remote data possession checking protocol in cloud storage," in *Algorithms and Architectures for Parallel Processing* (Lecture Notes in Computer Science), vol. 8631. Berlin, Germany: Springer-Verlag, 2014, pp. 611–617.
[16] H. Wang, "Proxy provable data possession in public clouds," *IEEE Trans. Services Comput.*, vol. 6, no. 4, pp. 551–559, Oct./Dec. 2013.
[17] H. Wang, "Identity-based distributed provable data possession in multicloud storage," *IEEE Trans. Services Comput.*, vol. 8, no. 2, pp. 328–340, Mar./Apr. 2015.
[18] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "FRR: Fair remote retrieval of outsourced private medical records in electronic health networks," *J. Biomed. Inform.*, vol. 50, pp. 226–233, Aug. 2014.
[19] H. Wang, "Anonymous multi-receiver remote data retrieval for pay-TV in public clouds," *IET Inf. Secur.*, vol. 9, no. 2, pp. 108–118, Mar. 2015.
[20] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. ASIACRYPT*, vol. 5350. 2008, pp. 90–107.
[21] Q. Zheng and S. Xu, "Fair and dynamic proofs of retrievability," in *Proc. CODASPY*, 2011, pp. 237–248.
[22] D. Cash, A. Küpçü, and D. Wichs, "Dynamic proofs of retrievability via oblivious RAM," in *Proc. EUROCRYPT*, vol. 7881. 2013, pp. 279–295.
[23] J. Zhang, W. Tang, and J. Mao, "Efficient public verification proof of retrievability scheme in cloud," *Cluster Comput.*, vol. 17, no. 4, pp. 1401–1411, 2014.
[24] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *J. Internet Technol.*, vol. 16, no. 1, pp. 171–178, 2015.
[25] T. Ma *et al.*, "Social network and tag sources based augmenting collaborative recommender system," *IEICE Trans. Inf. Syst.*, vol. E98-D, no. 4, pp. 902–910, 2015.
[26] K. Huang, J. Liu, M. Xian, H. Wang, and S. Fu, "Enabling dynamic proof of retrievability in regenerating-coding-based cloud storage," in *Proc. IEEE ICC*, Jun. 2014, pp. 712–717.
[27] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[28] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.
[29] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Trans. Services Comput.*, vol. 5, no. 2, pp. 220–232, Apr./Jun. 2012.
[30] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," *IEEE Trans. Services Comput.*, vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.