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

[1] K. Ravikumar
[1]Asst.professor,
Dept.of.Computer Science,
Tamil University, Thanjavur-613010

[2] I. Renuka
[2]Research Scholar,
Dept.of.Computer Science,
Tamil University, Thanjavur-613010

Abstract: More and more clients would like to store their data to public cloud servers (PCSs) along with the rapid development of cloud computing. 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. 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 are 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: identity-based proxy-oriented data uploading and 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 bilinear pairings. The proposed ID-PUIC protocol is provably secure based on the hardness of computational Diffie–Hellman problem. Our ID-PUIC protocol is also efficient and flexible. Based on the original client's authorization, the proposed ID-PUIC protocol can realize private remote data integrity checking, delegated remote data integrity checking, and public remote data integrity checking.

Keywords: *Cloud computing, Identity-based cryptography, Proxy public key cryptography, remote data integrity checking.*

*****

I. INTRODUCTION

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it.

It's called cloud computing because the information being accessed is found in "the cloud" and does not require a user to be in a specific place to gain access to it. This type of system allows employees to work remotely. Companies providing cloud services enable users to store files and applications on remote servers, and then access all the data via the internet.

1.1.BREAKING DOWN 'Cloud Computing'

In its essence, cloud computing is the idea of taking all the heavy lifting involved in crunching and processing data away from the device you carry around, or sit and work at, and moving that work to huge computer clusters far away in cyberspace. The internet becomes the cloud, and – your data, work and applications are available from any device with which you can connect to the internet, anywhere in the world. According to research conducted by business management consultant firm Forrester, the cloud computing market is anticipated to reach $191 billion by the year 2020.

1.1.1.Different Types of Cloud Computing

Cloud computing is not a single piece of technology, like a microchip or a cell phone. Rather, it's a system, primarily comprised of three services: infrastructure as a service (IaaS), software as a service (SaaS)+ and platform as a service (PaaS). SaaS is expected to experience the fastest growth, followed by IaaS.

Software as a Service (SaaS): SaaS involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This rapidly growing market could provide an excellent investment opportunity, with a Goldman Sachs report projecting that by 2018, 59% of the total cloud workloads will be SaaS.

Infrastructure as a Service (IaaS): Infrastructure as a service involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an outsourced, on-demand service.

Platform as a Service (PaaS): Of the three layers of cloud-based computing, PaaS is considered the most complex. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online, it is actually a platform for creating software that is delivered via the internet. A report by Forrester indicates that PaaS solutions are expected to generate $44 billion in revenues by the year 2020.

1.1.2.Cloud Advantages

The rise of cloud-based software has offered companies from all sectors a number of benefits, including the ability to use software from any device, either via a native app or a browser. As a result, users are able to carry over their files and settings to other devices in a completely seamless manner. Cloud computing is about far more than just accessing files on multiple devices, however. Thanks to cloud-computing services, users can check their email on any computer and even store files using services such as Dropbox and Google Drive. Cloud-computing services also make it possible for users to back up their music, files and photos, ensuring that those files are immediately available in the event of a hard drive crash.

Cloud computing offers big businesses some serious cost-saving potential. Before the cloud became a viable alternative, companies were required to purchase, construct and maintain costly information management technology and infrastructure. Now, instead of investing millions in huge server centers and intricate, global IT departments that require constant upgrades, a firm can use "lite" versions of workstations with lightning fast internet connections, and the workers will interact with the cloud online to create presentations, spreadsheets and interact with company software.

Individuals find that when they upload photos, documents, and videos to the cloud and then retrieve them at their convenience, it saves storage space on their desk tops or laptops. Additionally, the cloud-like structure allows users to upgrade software more quickly – because software companies can offer their products via the web rather than through more traditional, tangible methods involving discs or flash drives. In 2013, Adobe Systems announced all subsequent versions of Photoshop, as well as other components of its Creative Suite, would only be available through an internet-based subscription. This allows users to download new versions and fixes to their programs easily.

1.1.3.Disadvantages of Cloud Computing

With all of the speed, efficiencies and innovations of cloud computing come risks.Initially, security was seen as a detractor from using the cloud, especially when it came to sensitive medical records and financial information. While regulations are forcing cloud computing services to shore up their security and compliance measures, it remains an ongoing issue. Media headlines are constantly screaming about data breaches at this or that company, in which sensitive information has made its way into the hands of malicious hackers who may delete, manipulate or otherwise exploit the data (though, according to some reports, most of the data breeches have been with on-site systems, not those in the cloud). Encryption protects vital information, but if the encryption key is lost, the data disappears. Servers maintained by cloud computing companies can fall victim to a natural disasters, internal bugs and power outages, too. And unfortunately, the geographical reach of cloud computing cuts both ways: A blackout in California could paralyze users In New York; a firm in Texas could lose its data if something causes its Maine-based provider to crash. Ultimately, as with any new technology, there is a learning curve for employees and managers. But with many individuals accessing and manipulating information through a single portal, inadvertent mistakes can transfer across an entire system. One of the biggest impediments to cloud computing has been internet bandwidth: We needed the internet to be a super fast, rushing river, moving just as fast wirelessly as it does in the wired home or office. We're finally getting there with widespread broadband adoptions, and with 3G and 4G wireless technology. We've also had to wait for internet security standards and protocols to get solid enough to make CEOs feel safe exporting huge data clusters out of their buildings and into someone else's hands.

But now that they have, and realize the savings potential associated with the ability to outsource the software and hardware necessary for tech services, the pace at which businesses embrace and utilize internet-based systems has quickened. According to Nasdaq, investments in key strategic areas such as big data analytics, enterprise mobile, security and cloud technology, is expected to increase to more than $40 million by 2018.

1.1.4.The World of Business Cloud Computing

Businesses can employ cloud computing in different ways. Some users maintain all apps and data on the cloud, while others use a hybrid model, keeping certain apps and data on private servers and others on the cloud. When it comes to providing services, the big players in the corporate computing sphere include:

- Google Cloud
- Amazon Web Services
- Microsoft Azure
- IBM Bluemix
- Aliyun

Amazon Web Services (AWS) is 100% public and includes a pay-as-you-go, outsourced model. Once you’re on the platform you can sign up for apps and additional services. Google Cloud, which targets consumer banking and retail, is one of the latest entrants. Microsoft Azure, which recently launched U.K. data centers, allows clients to keep some data at their own sites.With cloud-based services expected to increase exponentially in the future, there has never been a better time to invest, but it is important to do so cautiously. (See A Primer On Investing In The Tech Industry.) In choosing cloud-based investment options, remember that there are many different elements involved in the sector, each of which presents an opportunity. Smaller companies that are focused solely on cloud computing tend to be more expensive relative to how much money they're making today. As such, they are a little riskier, but if cloud computing really takes hold – and all signs point toward widespread adoption – these more focused plays could outperform larger companies just dipping their toes in the water. But don't discount the potential positives that even a huge company like IBM or Microsoft could see. As large corporations start to crunch the numbers and see the potential savings of outsourcing parts of their IT divisions, some big orders could be coming the way of the tech sector's giants. Indeed, established computer companies, like U.S. software giant Oracle Corporation (NYSE:ORCL), are moving away from traditional software and diving into such cloud computing investments. Oracle picked up 3,600 customers and $690 million in its 2015 fourth-quarter revenue from its cloud-computing business. As five-star analyst Brian White of Cantor Fitzgerald commented, Oracle’s transition to the cloud “appears to be occurring much faster than the company anticipated.” One caveat: Since cloud computing is so hot right now, many a firm is eager to appear involved. Take the time to do due diligence to review exactly what it is that the company offers, and ensure that they are not simply using industry jargon to leverage market interest.

1.1.5.Hardware-Plays

Companies like Google (Nasdaq:GOOG), IBM (NYSE:IBM), Intel (Nasdaq:INTC), Microsoft (Nasdaq:MSFT), Cisco (Nasdaq:CSCO) and Hewlett-Packard (NYSE:HPQ) are making huge investments in cloud computing. They are building out the seas of servers that will make cloud computing possible. Some, like Google and Microsoft, have their own applications to offer over the internet, while firms like IBM and HP are more interested in providing the backbone to large corporate customers. Plenty of companies are building centralized data centers, too. Some are pioneers in the internet-provider industry, like Rackspace, which is owned by Apollo Global Management (NYSE: APO); others come from other areas of the web world, like Amazon.com (Nasdaq: AMZN). Though known to consumers as the internet superstore, Amazon is also a market leader in the cloud computing sector. The company continues to invest billions of dollars on the back end, expanding its AWS data centers across the country and around the world, and is reportedly working on a new cloud service focused on a branch of artificial intelligence called deep learning or machine learning (ML), which helps train computers to recognize speech, images and objects. There's also a realm of slightly smaller companies are working to upgrade the internet and the corporate IT center for cloud computing. Akamai (Nasdaq:AKAM) is hard at work making the internet's "pipes" more able to pump the huge amounts of data required to make cloud computing a reality.

Software-Plays

This trend won't just be about hardware. Software also has to be changed for cloud computing to work. Instead of installing software on your computer or huge IT staffs updating in-house server farms, software applications will be exclusively delivered and maintained over the internet. As mentioned earlier, Software as a Service is rapidly growing. Innovative companies like Salesforce.com (NYSE:CRM) and Concur Technologies (Nasdaq:CNQR) have taken popular applications like expense reporting, travel logistics, and contact management, and offered them as SaaS. While some of the best-known brands have been acquired and taken private (RIP Keynote Systems), you can sometimes invest in their parent company. Case in point: human resource management software provider Taleo, now owned by Oracle.

Vendors who specialize in cloud-based file-sharing and storage are another option. Apple (Nasdaq:AAPL) and Google are in the game, of course, as is Dropbox (currently private, but with rumors of an IPO swirling as of 2017) and Mozy, which is owned by EMC Corporation (NYSE: EMC). Security remains a vital concern when accessing files online. More and more companies are now providing cloud-security solutions, including Forcepoint (co-owned by Raytheon (NYSE: RTN) and Qualys (NASDAQ: QYLS). Cloud-based solutions often provide some type of desktop virtualization or application technology. Leading vendors providing virtualization technology include Citrix (Nasdaq: CTXS) and VMware (NYSE:VMW). You could even consider mobile internet devices as a good play on this trend. As devices like Research in Motion's (Nasdaq:RIMM) Blackberries or Samsung Electronics' (OTHEROTC: SSNFL) Galaxies offer more applications, they will make their way into many more hands this decade.

Once they get the green light to buy and then install such software – known as a cloud or multicloud management platform — organizations would do well to draft a deployment plan, advised the Cloud Standards Customer Council. The group, which works on establishing standards for the cloud industry, hosted a webinar on understanding and evaluating cloud management software in late July.

The key deployment question organizations should entertain is whether to buy traditional software, which would reside on their own servers or a prepackaged software-as-service (SaaS) offering. IBM cloud expert Mike Edwards spoke in the webinar about the two offerings. Subscribing to cloud software takes away the burden of having people in-house who “understand how to do that installation, how to install the bits and then run it.” But a SaaS application won’t fit every business situation.

II. 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.

2.1.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*.

III. 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.

3.1.Advantages of Proposed System:

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

IV. SYSTEM ARCHITECTURE

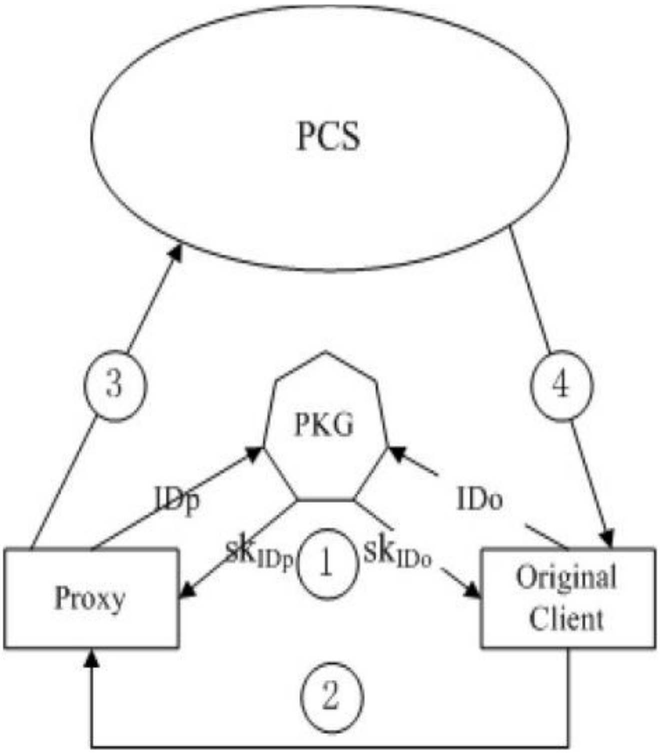

Fig. 1. Architecture of our ID-DPDP protocol.

V. MODULES

1. Original Client Module
2. Public Cloud Server Module
3. Proxy Module
4. Key Generation Center (KGC) Module

Module Description:

Original Client:

An entity, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.

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.

Proxy:
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_ω which is signed and issued by Original Client, it can process and upload the original client's data; otherwise, it cannot perform the procedure.

KGC (Key Generation Center):
An entity, when receiving an identity, it generates the private key which corresponds to the received identity.

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.

REFERENCE

[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.