IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 5 (May. 2019), ||S (XI) || PP 16-22

An Efficient Cloud based Revocable Identity-Based Encryption in Cloud Data Security Authentication and Data Sharing

Nikita Daudkar[1],Pranjal Dhore[2], Nisha Balani[3]
[1]*MTech. Jhulelal institute of technology, Nagpur, Maharashtra, India*
[2]*Tantransh Solutions, Nagpur, Maharashtra, India*
[2]*Asst. Professor, Computer Science Engineering, jhulelal institute of technology, Nagpur, Maharashtra, India*

Abstract : *With the rapid development of network bandwidth, the volume of user's data is rising geometrically. User's requirement cannot be satisfied by the capacity of local machine any more. Therefore, people try to find new methods to store their data. Cloud storage is a cloud computing system which provides data storage and management service. With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together coordinately. Nowadays there are a lot of companies providing a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Amazon Web Services, etc. These companies provide large capacity of storage and various services related to other popular applications, which in turn leads to their success in attracting humorous subscribers. However, cloud storage service still exists a lot of security problems. The privacy problem is particularly significant among those security issues. Apples iCloud leakage event in 2014, numerous Hollywood actresses private photos stored in the clouds were stolen. This event caused an uproar, which was responsible for the users' anxiety about the privacy of their data stored in cloud server. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability. Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more—over the Internet ("the cloud") to offer faster innovation, flexible resources and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change. Azure is Microsoft's cloud platform, just like Google has it's Google Cloud and Amazon has it's Amazon Web Service or AWS.000. Generally, it is a platform through which we can use Microsoft's resource.*

Keywords: *Azure Microsoft Cloud Computing, Cloud Storage, Anonymity*

I. Introduction

Storing and exchange of data in cloud computing become the necessity of modern working pattern in IT industry. Cloud computing provides multitudinous benefits to both service provider and customer. However, the security of cloud computing has been a challenging one. To increase security and confidentiality of data in cloud environment, recent years witness the development of cloud computing technology .With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. However, in current storage schema, user's data is totally stored in cloud servers. In other words, users lose their right of control on data and face privacy leakage risk. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. Microsoft Azure, formerly known as Windows Azure, is Microsoft's public cloud computing platform. It provides a range of cloud services, including those for compute, analytics, storage and networking. Users can pick and choose from these services to develop and scale new applications, or run existing applications, in the public cloud. It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfills the aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period. As indicated n Figure 1, a RIBE-based data sharing system works as following steps :

1. The data provider (e.g., David) first decides users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the cipher text of the shared data to the cloud server.
2. When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding cipher text. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.
3. In some cases, e.g., Alice's authorization gets expired, David can download the cipher text of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

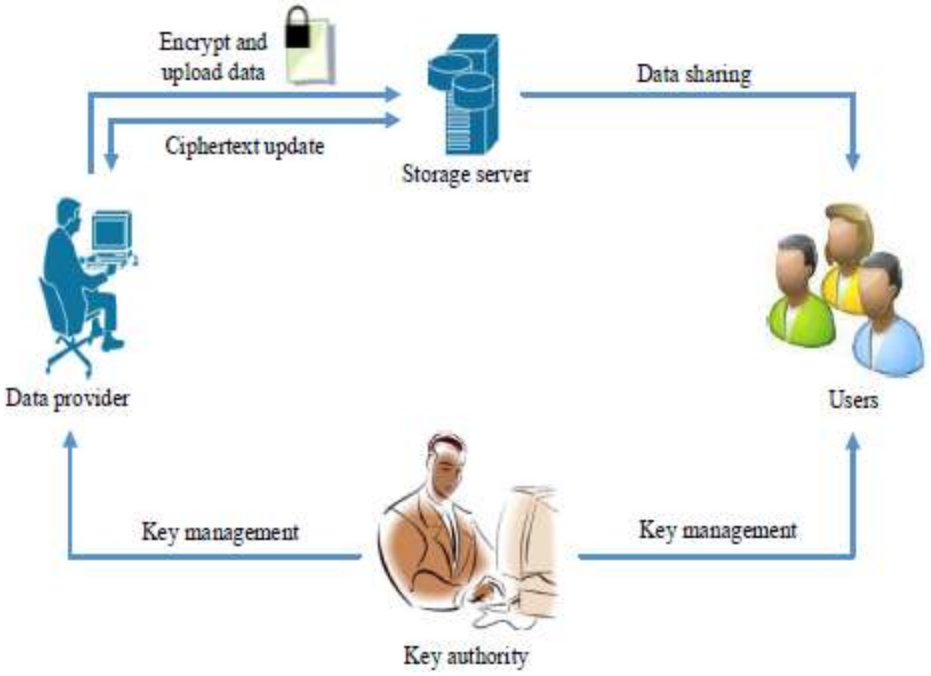


Fig. 1. A natural RIBE-based data sharing system

Obviously, such a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the cipher text periodically by using secret key. Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-encrypt- upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage. One method to avoid this problem is to require the cloud server to directly re-encrypt the cipher text of the shared data. However, this may introduce cipher text extension; namely, the size of the cipher text of the shared data is linear in the number of times the shared data have been updated. In addition, the technique of proxy re-encryption can also be used to conquer the aforementioned problem of efficiency. Unfortunately, it also requires users to interact with the cloud server in order to update the cipher text of the shared data.

- **Data confidentiality**: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.
- **Backward secrecy**: Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

- **Forward secrecy**: Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.
- **Authentication cryptography:** Clients using cloud must be encrypted to protect their profile authentication along with data they share onto cloud.

a. **Microsoft Windows Azure**

i. It is Microsoft cloud operating system where we will share data

ii. We will use SQL Azure for database management system

iii. We will use Azure security for user management

b. **Authentication Cryptography**

i. User's Profile Data will be stored in encrypted format to improve data security. Only authenticated and properly decrypted user can share and receive data.

ii. We will maintain key to share and receive data.

c. **RS-IBE RESISTANT TO DECRYPTION KEY EXPOSURE**

i. We first will present a concrete construction of RSIBE resistant to decryption key exposure, and then discuss its security and performance.

d. **Security Analysis**

i. If there exists a PPT adversary A breaking the INDRID- CPA security of the proposed RS-IBE scheme, then there exists an algorithm C solving the decisional ℓ-BDHE problem such that

$$\mathbf{Adv}_{\mathcal{C}}^{\ell\text{-dBDHE}}(\lambda) \geq \frac{1}{32Tq^2(n+1)} \cdot \mathbf{Adv}_{\text{RS-IBE},A}^{\text{IND-RID-CPA}}(\lambda, T, N)$$

Where q is the maximum number of secret key queries and decryption key queries, and
T = 2ℓ is the total number of time periods.
Proof. Given a PPT adversary A breaking the IND-RIDCPA security of the proposed RS-IBE scheme, we will construct an algorithm C to solve the decisional ℓ-BDHE problem. More precisely, given a random instance of ℓ-BDHE problem in the form of a tuple (G1,G2, e, p, **f**,D)where **f** = (g, gs, f1, ..fℓ, fℓ+2, ..., f2ℓ) and fi = gai∈G1 for≤ i≤ 2ℓ, the algorithm C can decide if D = e(fℓ+1, gs) by simulating the experiment according to the following steps.

II. Implementation Detail of Workflow

2.1 Access Cloud Computing

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

KPMG has taken this definition as a starting point and has narrowed it somewhat to the perspective of a recipient of cloud services.

Cloud computing differs from traditional IT via the following characteristics:

- *Multi-tenancy. Unlike traditional IT, the IT resources in the cloud are shared across multiple users.*
- *Paid services. The user only pays for the use of cloud services and does not invest in additional hardware and software.*
- *Elasticity. The capacity can either increase or decrease at all times.*
- *Internet dependent. The primary network for cloud services is the Internet.*
- *On-demand services. Unlike the greater part of traditional IT, cloud services can be utilized practically immediately."*

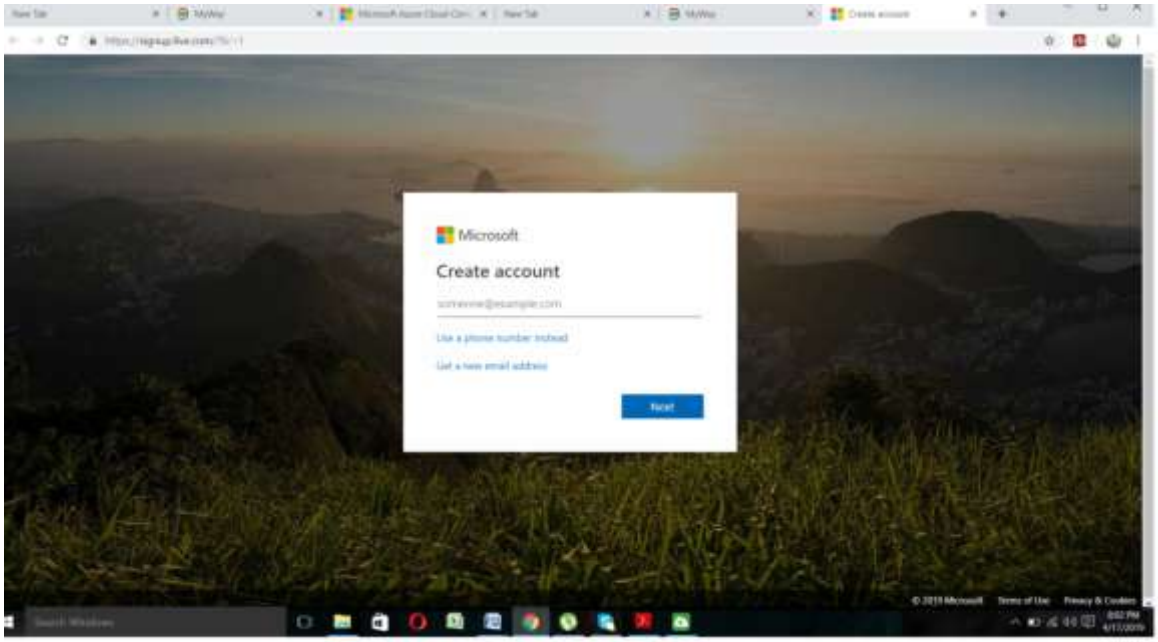
Different types of cloud services are available. First and foremost is Software-as-a-Service (SaaS) where software is provided as a cloud service. There is also Platform-as-a-Service (PaaS) where a platform (operating system, application framework, etc.) is offered as a cloud service. Finally, there is Infrastructure-as-a-Service

(IaaS) where an IT infrastructure or part thereof (storage, memory, processing power, network capacity, etc.) is offered as a cloud service.

Figure 1. Forms of cloud computing.

2.2 Create an account in hotmail

When user used to Microsoft windows azure cloud computing. First to create an account in hotmail Then hotmail id used in windows azure cloud computing.



2.3 Microsoft windows azure

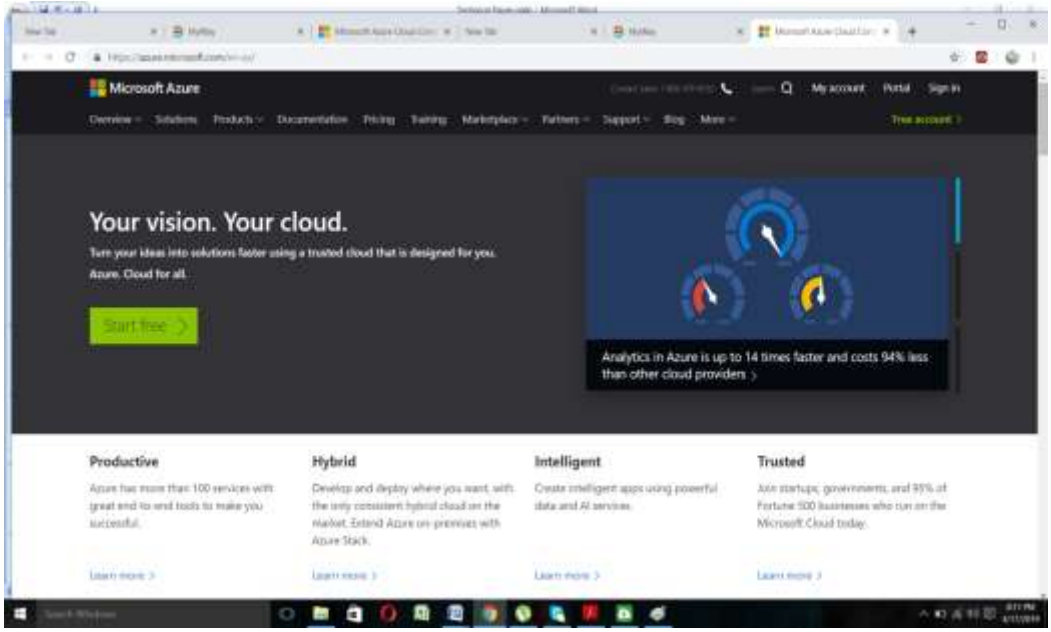
Microsoft Azure, formerly known as Windows Azure, is Microsoft's public cloud computing platform. It provides a range of cloud services, including those for compute, analytics, storage and networking. Users can pick and choose from these services to develop and scale new applications, or run existing applications, in the public cloud. For example, to set up a huge server, we will require huge investment, effort, physical space and so on. In such situations, Microsoft Azure comes to our rescue. It will provide us with virtual machines, fast processing of data, analytical and monitoring tools and so on to make our work simpler. The pricing of Azure is also simpler and cost-effective.

Some following are the services of Microsoft Azure offers:

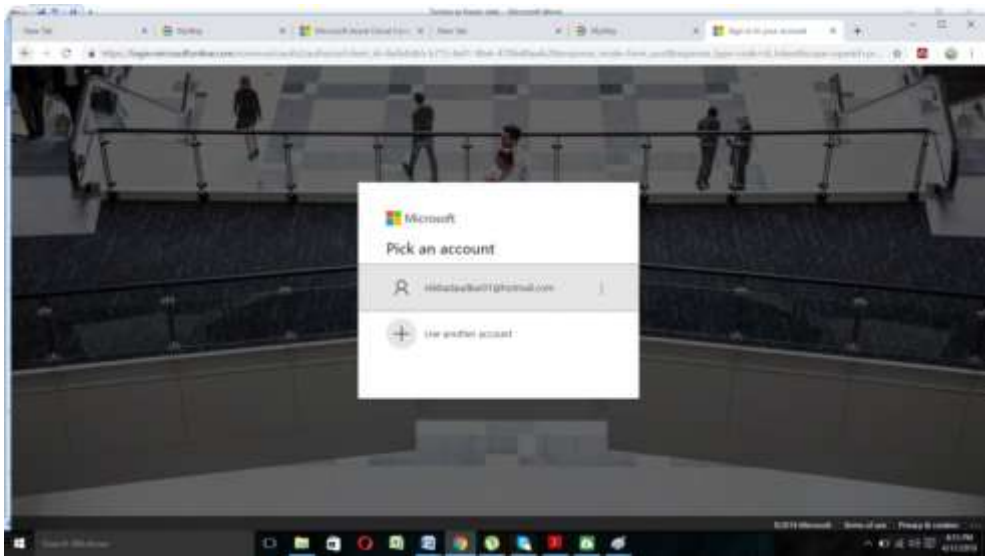
1. **Compute:** Includes Virtual Machines, Virtual Machine Scale Sets, Functions for serverless computing, Batch for containerized batch workloads, Service Fabric for micro services and container orchestration, and Cloud Services for building cloud-based apps and APIs.
2. **Networking:** With Azure you can use variety of networking tools, like the Virtual Network, which can connect to on-premise data centers; Load Balancer; Application Gateway; VPN Gateway; Azure DNS for domain hosting, Content Delivery Network, Traffic Manager, Express Route dedicated private network fiber connections; and Network Watcher monitoring and diagnostics
3. **Storage:** Includes Blob, Queue, File and Disk Storage, as well as a Data Lake Store, Backup and Site Recovery, among others.
4. **Web + Mobile:** Creating Web + Mobile applications is very easy as it includes several services for building and deploying applications.
5. **Containers:** Azure has a property which includes Container Service, which supports Kubernetes, DC/OS or Docker Swarm, and Container Registry, as well as tools for micro services.
6. **Databases:** Azure has also includes several SQL-based databases and related tools.
7. **Data + Analytics:** Azure has some big data tools like HDInsight for Hadoop Spark, R Server, HBase and Storm clusters
8. **AI + Cognitive Services:** With Azure developing applications with artificial intelligence capabilities, like the Computer Vision API, Face API, Bing Web Search, Video Indexer, Language Understanding Intelligent.
9. **Internet of Things:** Includes IoT Hub and IoT Edge services that can be combined with a variety of machine learning, analytics, and communications services.
10. **Security + Identity:** Includes Security Center, Azure Active Directory, Key Vault and Multi-Factor Authentication Services.
11. **Developer Tools:** Includes cloud development services like Visual Studio Team Services, Azure DevTest Labs, HockeyApp mobile app deployment and monitoring, Xamarin cross-platform mobile development and more.

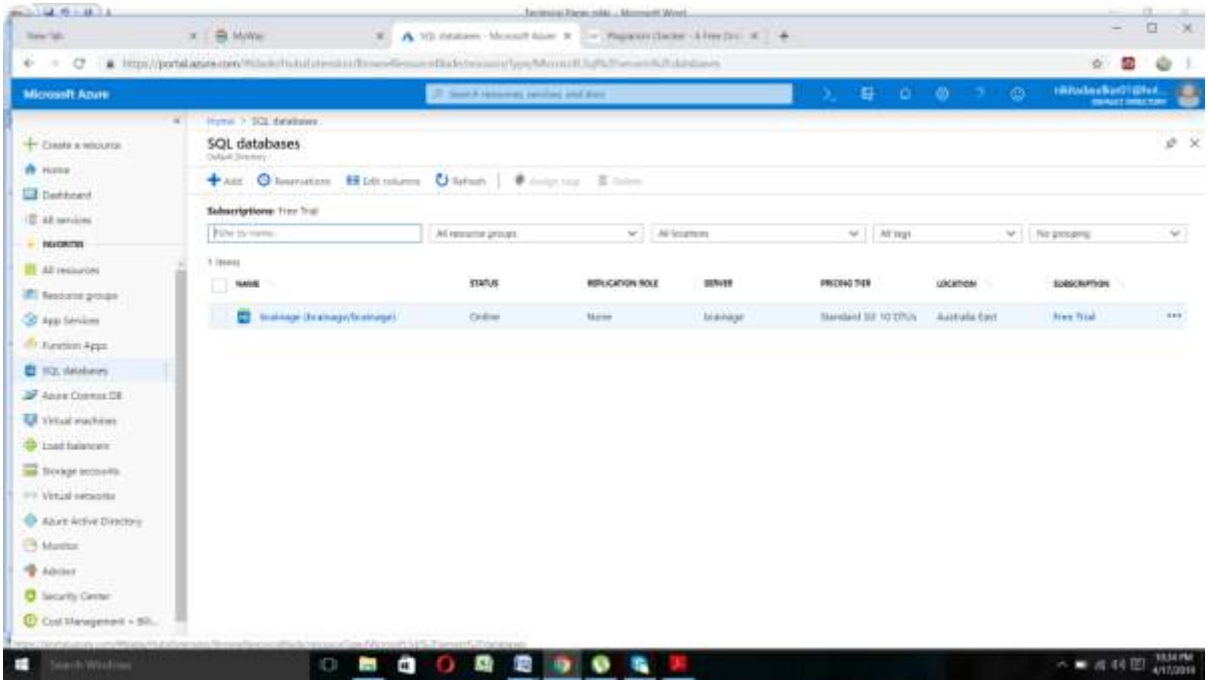
Difference between AWS (Amazon Web Services), Google Cloud and Azure

	AWS	Google Cloud	Azure
Technology	EC2 (Elastic Compute Cloud)	Google Compute Engine (GCE)	VHD (Virtual Hard Disk)
Databases Supported	AWS fully supports relational and NoSQL databases and Big Data.	Technologies pioneered by Google, like Big Query, Big Table, and Hadoop, are naturally fully supported.	Azure supports both relational and NoSQL databases, and Big Data, through Windows Azure Table and HDInsight.
Pricing	Per hour – rounded up	Per minute – rounded up (minimum 10 minutes)	Per minute – rounded up commitments (pre-paid or monthly)
Models	On demand, reserved, spot	On demand – sustained use	On demand – short term commitments (pre-paid or monthly)
Difficulties	Many enterprises find it difficult to understand the company's cost structure	Fewer features and services.	Less "enterprise-ready"
Storage Services	• Simple Storage Service (S3) • Elastic Block Storage (EBS) • Elastic Block Storage (EBS)	• Blob Storage • Queue Storage • File Storage • Disk Storage • Data Lake Store	• Cloud Storage • Persistent Disk • Transfer Appliance
Machine Learning	• Sage Maker • Lex • Polly • And many more	• Machine Learning • Azure Bot Service • Cognitive Service	• Cloud Speech API • Cloud Video Intelligence • Cloud Machine Learning Engine



In the above screenshot user login to Microsoft azure cloud computing and click on start free button. Then pick an account using hotmail id and to click azure portal then click on create SQL databases.





III. Conclusions

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in this parathion of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, Cloud computing brings great convenience for people. We proposed a notion called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. Cloud Computing allows companies to use available resources at any time without a limit. The sensitive information is also transmitted and stored in the cloud at lower cost. However, the prevalence of cloud is suffered by its security challenges. To improve the security of cloud computing the new model has been proposed.

References

[1]. Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/
[2]. Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/
[3]. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.
[4]. G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.
[5]. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.
[6]. J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction,"in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.