

A Secure Electronic Student Record using Hierarchical Identity-based Authentication over University Cloud Storage

Hazem A. Elbaz¹, Mohammed H. Abd-elaziz¹, Taymoor Nazmy¹

1 Ain-Shams University – Cairo, Egypt, Faculty of Computer Science and information system
hazem.baz@gmail.com

2 Ain-Shams University – Cairo, Egypt, Faculty of Computer Science and information system
mhashem100@yahoo.com

3 Ain-Shams University – Cairo, Egypt, Faculty of Computer Science and information system
ntaymoor19600@gmail.com

ABSTRACT

Cloud computing is a state-of-the-art technology to build a storage platform for data backup, resource sharing, file synchronization, etc. there for modern university environments, university providers are more willing to move their electronic student record systems to cloud. This archetype enable to achieve better interoperability and lower operational cost with other university providers, instead of building and maintaining dedicated data centers. However, many security challenges associated with authentication, identity management, access control, trust management, and so on, may raise in the adaptation of cloud computing in electronic student records (ESR) systems. To satisfy these requirements, we present the hierarchy feature of the hierarchical identity based authentication (HIBA) and key agreement to propose a systematic access control mechanism to support sharing data of (ESR) aggregated from various university providers in clouds as an application. The feasibility and efficiency of our approach demonstrate by implementing a concept prototype along with security evaluation.

Key words: Cloud Security, Cloud Authentication, Cloud Storage, Hierarchical Identity-Based, Key Agreement.

INTRODUCTION

In the earlier days, the student record details were written and maintained in the paper by the registration department, finance department, academic affairs, etc. Because of the technological improvements in the Information Technology, the data can be saved at various places like desktop, Laptop and some secondary devices like compact disk, etc. Nowadays, the advance in computer technology has progressed to an extent of storing the information to the cloud, which helps the university's employees, and students to access the information

when it is needed. Electronic Student Record (ESR) is one of the major services provided by the cloud. ESR is a collection of student documents related information that is documented maintained by the student. The goal of ESR is to provide university details about the student[1].

As a result, we can found student's ESRs scattered throughout the entire university departments. From a university point of view, in order to provide quality care for students, it is important to gain access to information integrated student information that is often collected at the point of university to ensure the freshness of the data time-sensitive. An efficient, secure and low-cost mechanism is required for sharing ESRs among multiple university providers. However, in current university settings, university providers mostly establish and maintain their own electronic student record (ESR) systems for storing and managing ESRs. It is expensive for university providers to make self-managed data centers. Besides, it is extremely slow and costly to share and integrate of ESRs among ESR systems managed by different university providers. Such use is effective and low fashion cost-effective to become the biggest obstacles to move forward the university care information technology industry. A common and open infrastructure platform can play a vital role in addressing and changing such a situation.

This model shifts the site of computing infrastructure to third-party service providers that handle the management of HW and SW resources. It has shown enormous potential to enhance collaboration, scale, agility, cost efficiency and availability. As such, university providers willing to shift their ESR systems into clouds instead of building and maintaining dedicated data center. The cloud storage services should enhance with a secure access control scheme and encrypt plain data into ciphertext, by applying the confidential protocol and privacy policy. In charge of managing Cloud data utilization and security is the hierarchical access control scheme that comprise the hierarchical users and their access privilege assignments. Therefore, in our Cloud storage service, we are working on an efficient identity based authentication for access control scheme to regularize user privileges[2].

The reset of this paper organizes as follows: Section 2 presents concepts of identity-based cryptography and hierarchal identity based cryptography. Section 3 gives introduction to cloud storage security, what the threads it face and solutions. Section 4 shows our proposed solution. Section 5 Evaluation of proposed work. Section 6 concludes the paper and outline for future research.

IDENTITY BASED CRYPTOGRAPHY

Identity-based cryptographic (IBC) scheme [10] is a kind of public-key based approach, in which user's identity is use as the public key. The use of identity-based cryptography as the basis of a security infrastructure is beneficial whenever in a dynamic environment, many parties want to communicate with each other and the communications endpoint addresses are already known or a secure naming service exists [4, 5]. Compared with traditional public- key systems, such as PKI, IBC has some advantages, especially for large-scale distributed applications. The advantages of it cannot only reduce message transmission but also can avoid disclosing session key during transmission. Another advantage of identity-based encryption

is that encryption and decryption can be conducted offline without the generation center. Hierarchical identity- based cryptography (HIBC) has been proposed in [6] to improve the scalability of the standard IBC scheme, in which multiple KGCs are used to cooperatively allocate hierarchical identities to users in their domains. Recently IBC and HIBC have been proposed to provide security for some Internet applications.[7] For example, applying IBC in the grid computing and cloud computing security has been explored in [8, 9]. In the following, we briefly introduce the mathematical concepts that are required in this paper.

Bilinear pairings:

Bilinear pairings are the most commonly used primitives in IBC and HIBC.

Let $G1$ be an additive cyclic group of large prime order q , $G2$ be a multiplicative cyclic group of the same order and P be a generator of $G1$. A cryptographic bilinear map e is defined as $e: G1 \times G1 \rightarrow G2$ with the following properties:

Bilinear: $e(aR, bS) = e(R, S)^{ab} \forall R, S \in G1$ and $a, b \in Z^*_q$.

Non-degeneracy: For each $R \neq O \in G1$, there exists $S \in G1$ such that $e(R, S) \neq 1$, where O is the identity element in $G1$ and 1 is the identity element in $G2$.

Computable: There exists an efficient algorithm to compute $e(R, S) \forall R, S \in G1$.

In general, implementation, $G1$ is the group of points on an elliptic curve and $G2$ denotes a multiplicative sub-group of a finite field. Typically, the mapping e is derive from either the Weil or the Tate pairing on an elliptic curve over a finite field. We refer to [10] for more comprehensive description on how these groups, pairing and other parameters are defined.

Computational problems:

Here, we present some computational hard problems, which will form the basis of security of IBC and HIBC.

Discrete Logarithm Problem (DLP): Given two elements $R, S \in G1$, find an integer $a \in Z^*_q$, such that $S = aR$ whenever such an integer exists.

Computational Diffie-Hellman Problem (CDHP): For any $a, b \in Z^*_q$, given $\langle P, aP, bP \rangle$, compute abP .

Decisional Diffie-Hellman Problem (DDHP): For any $a, b, c \in Z^*_q$, given $\langle P, aP, bP, cP \rangle$, decide whether $c \equiv ab \pmod q$.

BilinearDiffie-HellmanProblem(BDHP): For any $a, b, c \in Z^*_q$, given $\langle P, aP, bP, cP \rangle$, compute $e(P, P)^{abc}$.

GapDiffie-HellmanProblem(GDHP): A class of problems, where DDHP can be solved in polynomial time but no probabilistic polynomial time algorithm exists which can solve CDHP.

In this paper, we propose hierarchical identity-based authentication key management protocol. The use of an identity-based authentication scheme indeed improves the efficiency of achieving confidentiality and authenticity in key management of the cloud computing. It can effectively decrease the computational costs and communication overheads in comparison with the identity-based encryption key management schemes. It also can solve the scalability problem in cloud computing environment.

CLOUD STORAGE SECURITY

Cloud computing has emerged as feasible and readily available platform to a wide range of users like individuals, businesses and governments. Most of enterprises, startups and Data Owners store their sensitive and confidential data on cloud to reduce the investment on software, hardware and storage media, they may not have enough finance to purchase resources or ensure necessary security. Other reason to use the advantage of pay-per-use feature of cloud computing. A key for backup outsourcing of any enterprises or government agencies is Cloud storage. Traditionally, the data centers are the place of data owners archive their data. Where, their data volume is huge; therefor the investment of management is very expensive. Significantly, they are migrating to cloud for storing their data. To reduce the capital expenditure on resources. The users can access data from any location. Hence, cloud storage is more versatile and suitable for well-established businesses.[13]

Cloud data storage consists of a huge number of storage devices that distributed throughout the network; the structure of cloud data storage include distributed file system, resource pool, service interfaces and service level agreements. Cloud storage defined as a branch of infrastructure as a service (IaaS) in cloud computing, where its advantage is to provide the data, and by storing data remotely is reducing infrastructure costs [15]. Operates data storage cloud to provide storage service to different levels of customers as the cost of storage space required depends on the capacity and bandwidth.[14]

The security is the major issue in adopting cloud. We need some mechanisms to ensure that our data is stored in secured manner without any unauthorized access. Providing integrity to the data that has distributed over cloud is a challenging one. Security for the data stored in the cloud environment [16] is a wanted one. There is complementary and interoperability relationship between cloud data storage and cloud data storage security to make data in warehouse more secure.

We can divide cloud storage in two type [17]:

- 1- Designed cloud storage using technologies of encryptions and does not has theoretical framework for encryption.
- 2- Designed cloud storage using technologies of encryptions and does has theoretical framework for encryption.

In this paper, we will focus in cloud infrastructure as a service (IaaS) and on confidentiality for data that stored in cloud data storage by using Hierarchical identity-based authentication techniques as shown in figure(1).

Protected data from unauthorized access is the aim of secure storage. The risk on the secure storage is come from inside or the threat from outside. The secure storage is the main risk that make companies do not tend to cloud computing.

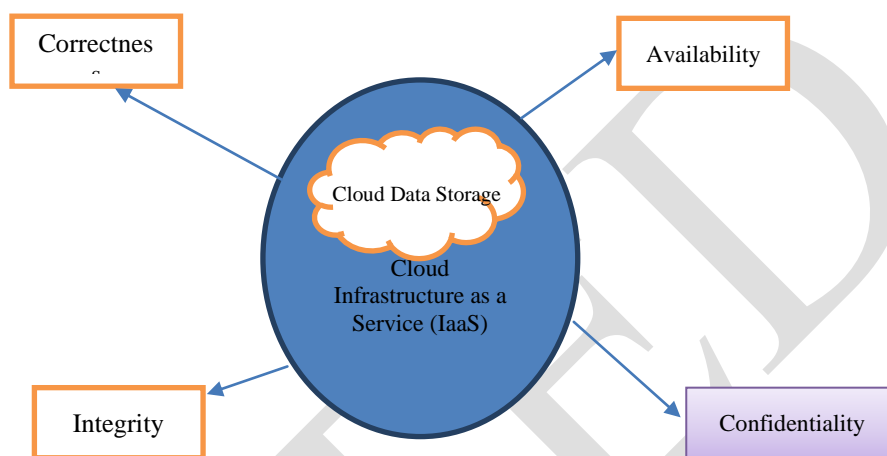


Fig (1): security policies for cloud computing

Data security mechanism such as audit, authority, certificate, and encryption are the content the safe storage media in cloud data security.

PROPOSED SOLUTION

Domain Problem:

A data security perspective has always been an important aspect of quality of service, cloud data storage face new challenging security treats for number of reasons. Firstly, because of the user loss control of data under cloud data storage, traditional cryptography primitives for the aims of data security protection cannot be adopted. Therefore, authentication and verification of correct data storage in the cloud must conduct without explicit knowledge of the whole data. The problem of authenticating and verifying correctness of data storage in the cloud becomes even more challenging, where various kinds of data for each user stored in the cloud and the demand of long-term continuous assurance of their data safety. Secondly, To ensure storage correctness and integrity authorized user will be allowed to access/modify the data, where the data stored in cloud data storage frequently updated by user, including insertion, deletion, modification, appending, reordering, etc.

The main problem here is that this digital identity can only use in one cloud, private one or public one. Users in a hybrid cloud may be want to access services that provided by different clouds, so it need multiple identities for each one of services on these clouds. Here is show clearly not user friendly. In this paper, we propose a system for cloud data storage where each user and server will have its own unique identity, with this unique, the key distribution and mutual authentication can be greatly simplified.

This paper was proposed to solve this problem by using identity management in clouds data storage with hierarchal identity based cryptography, where this proposed scheme allow users from one cloud to access to service in other one with single digital identity, and also allow them in hybrid cloud to simplified a mutual authentication and key distribution. Our protocol design should achieve the following security and performance guarantee, to enable privacy-preserving public accessing for cloud data storage. Our ideas can summarize as follows:

- 1- Storage correctness: to ensure that there exists no cheating cloud server that can pass the access from user access, without indeed storing users' data intact.
- 2- Privacy preserving: to ensure that there exists no way for user access to derive users' data content from the information collected during the accessing process.
- 3- Batch accessing: to enable user access with secure and efficient accessing capability to cope with multiple accessing delegations from possibly large number of different users simultaneously.
- 4- Lightweight: to allow user access to perform accessing with minimum communication and computation overhead.

Our Solution:

in this paper, to achieve an efficient identity based authentication system for cloud data storage security, we utilize the protocols based on identity-based encryption (IBE) while keeping all above requirements in mind, and allowing flexible access to stored data. We further explore the technique of identity-based signature (IBS) to extend our main result into a multi-user setting, to support efficient Handling of multiple accessing tasks, where user access can perform multiple accessing tasks simultaneously.

To deal with this security issue we enhance using identity based authentication. It gives the following advantages ability to share, between internal networks and external networks and enables the portability of identity information to access to different networks, increases the security of networks, where it needs a user to identity and authenticate himself to the system for one time, and his identity information will be used in different networks. Trusting identity also makes users from different networks to trust each other.

This paper propose to use identity-based management with HIBC at cloud data storage. PKGs will acts as PKGs in identity based cryptography system and allocate hierarchal identities to users in sub-domains. Each cloud data storage has root in overall domain, and within this cloud, each sub-domain (private or public) has also its PKG. the role of root PKG is manage whole cloud data storage, the first level contains the private clouds or public clouds, second level it contains users and servers. Allocating and authenticating identities for all clouds (private or public) also done by root PKG. The hierarchical identity-based key management scheme is composed of three levels using authentication algorithm. The top level is root PKG. The level-1 is domain PKGs, which are the cloud services in the cloud computing. The level-2 is users in the cloud computing. The user's public key consists of their identity and their domain's identity. For example, the cloud service identity is ID1, the user M's identity is IDm, and the identity of user M in hierarchical key management system is $ID1 \parallel IDm$.

For example, root PKG creates identity ID_Uni to a private cloud of a University. Identities of all users and servers in a private cloud or public cloud manage and allocate by using sub-domain PKG. A hierarchal identity created for user and server, which is combine both identity of the user or server and the identity of the sub- domain. For example, the identity of email

server in the private cloud of a University can be ID_Uni.email_server. (may be need to make draw)

The Figure 2 shows the hierarchical PKGs architecture in cloud computing as follows:

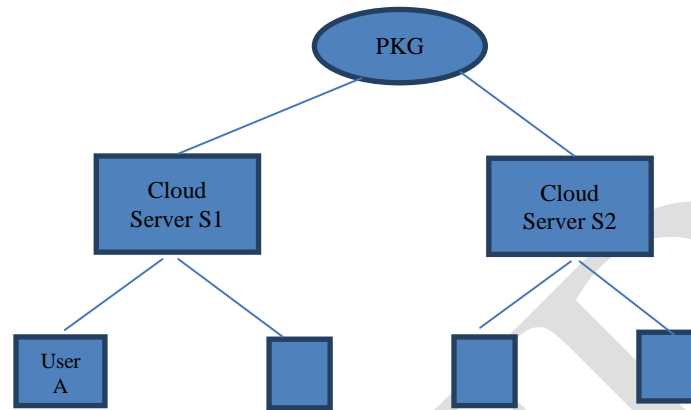


Fig (2): Hierarchical PKGs architecture in cloud computing

Key generation:

Root Setup: The root PKG operate as follow:

Step 1: Generate two cyclic groups G_1, G_2 of large prime order q and bilinear map $e:G_1 \times G_1 \rightarrow G_2$, chooses an arbitrary generator $P_0 \in G_1$;

Step 2: Root PKG picks a random $s_0 \in \mathbb{Z}_q^*$ and sets $Q_0 = s_0 P_0$. Choose two hash functions: $H_1: \{0,1\}^* \rightarrow G_1, H_2: G_2 \rightarrow \{0,1\}^n$. The root PKG's secret is s_0 . The system public parameters are $(G_1, G_2, e, P_0, Q_0, H_1, H_2)$.

Lower-level setup: level-1 set up. The level-1 is cloud services. The cloud server S1 is the domain PKG. The cloud server S1 identity is ID_1 , then it picks a random $s_1 \in \mathbb{Z}_q^*$ and keeps it secret. To obtain the cloud service, let S_0 be the identity element of G_1 . The root PKG that is the cloud server S1 parent operates as follow:

Step 1: computes $P_1 = H_1(ID_1) \in G_1$;

Step 2: set the cloud server S1 private key $S_1 = s_0 P_1$;

Level-2 set up. Level-2 is the users. The user's private key is extracted in this phrase. Let 2-tuple (ID_1, ID_A) be an identity of Level-2 user A. The cloud server S1 which is the user's parent generates the private key as follows:

Step 1: computes $P_A = H_1(ID_1 || ID_A) \in G_1$;

Step 2: sets the user's private key $S_A = s_0 P_1 + s_1 P_A$;

Step 3: also gives the user the values of $Q_1 = s_1 P_0$ as "verification points" to the user and needs to return (S_A, Q_1) .

Key agreement and authentication algorithms:

Key agreement:

Alice and Bob wish to establish shared key. Each of them choose a random element as private key $a, b \in \mathbb{Z}_q^*$, and compute the values of corresponding element as public keys $W_A = aP_A, W_B = bP_B$ and $S_1 = s_0 P_1$. They can exchange the public keys as following:

Alice send a message M_1 to Bob contains W_A . Bob send a message M_2 to Alice W_B . Then they may produce the algorithm. Where Alice computes:

$$\begin{aligned}K_{AB} &= e(SA, WB + aPB) / e(S1, WB + aPB) \\ &= e(s0P1+s1PA, WB + aPB) / e(s0P1, WB + aPB) \\ &= e(s1PA, WB + aPB) \\ &= e(s1PA, bPB + aPB) \\ &= e(PA, PB)^{s1(a+b)}\end{aligned}$$

In addition, Bob computes:

$$\begin{aligned}K_{BA} &= e(WA + bPA, SB) / e(WA + bPA, S1) \\ &= e(WA + bPA, s0P1 + s1PB) / e(WA + bPA, s0P1) \\ &= e((a+b)PA, s1PB) \\ &= e(PA, PB)^{s1(a+b)}\end{aligned}$$

If Alice and Bob follow the algorithm, then they get the same share key.

An authentication:

Alice and Bob want to authenticate each other. They do as the follow:

Alice choose random element $a \in Z_q^*$, and computes $X = aP0$. Alice sends X to Bob, Bob sends $Y = e(X, SB)$ to Alice, then Alice computes Y . if $Y = e(X, s0P1 + s1PB) = e(aP0, s0P1 + s1PB) = e(aP0, s0P1)e(aP0, s1PB) = e(aQ0, P1)e(aQ1, PB)$. Therefore, Bob is a user cloud. On the other hand, it is not, Alice will refuse the Bob Communication.

EVALUATION OF PROPOSED WORK

Here, we will evaluate our proposed mutual authentication mechanism is secure against following attacks:

- **Known-key secrecy:** Key session between user and cloud data storage is compromise, which does not mean to compromise of other session keys because every session key evolves random values a and b , where a and b are selected arbitrary independently for each session by Alice and Bob respectively.
- **Replay Attack:** The most common attack in authentication process is Reply attack. However, random number mechanism and time-stamp in other protocols are the common countermeasures. In our scheme, we adopt the random number mechanism as a countermeasure. The messages, in phase $A \rightarrow B$ and $B \rightarrow A$ are with random number mechanism; therefore, replay attack could not work in any phase.
- **PKG forward Secrecy:** If the PKG's master key $s0$ compromise. Then the private keys of A and B cannot even compute by an adversary. As, private keys of A and B , it includes random values $a, b \in Z_q^*$. In addition, to compute session key K_{AB} , computation of $abP0$ is required. However, to compute $abP0$ for given $\langle P0, aP0, bP0 \rangle$ is equivalent to CDH problem on ECC.
- **Man in the Middle Attack:** User and server authenticate each other without knowing. An adversary or malicious PKG can try man in the middle attack by sending the forge message. However, to authenticate each other user and server exchange shared key for authentication. To compute shared key, knowledge of session keys is required, although, session key is assume secret and cannot be achieved with publicly known values as discussed above.
- **Scalability:** Hierarchical organization of our scheme can be scalable to mutli-level hierarchies. It can go beyond two levels by adding subdomains, sub-sub-domains, and so an. This satisfies the requirements of key management in cloud computing. However, the

message expansion factor and complexity of decryption grow only linearly with the number of levels in the hierarchy.

Our proposed algorithm is secure, because it has hierarchical design. Regular identity-based cryptography has one PKG that distributes private keys to users. If the root PKG exposes the private key, all users' private keys are also revealed. Our proposed algorithm 2-level users cannot influence if the root PKG reveals all private keys. Since they have different parents, the user's private keys are secure. In addition, any other domain that is not connected with the root PKG cannot expose their domain private keys. So it can greatly reduce the workload, also can allow key escrow at several levels.

CONCLUSION

Security in cloud data storage has some disadvantages in key management and authentication. This paper presented an introduction of cloud data storage security problems, concepts of hierarchical identity-based management and how it is suitable to solve the problem in cloud data storage authentication. We proposed using an efficient identity-based management and HIBC in cloud data storage, explained how the system can generate and distribute the public and private keys to users and servers of data stored in cloud. In addition, we showed how two parties in the cloud data storage can generate a secret shared key without certificate (message exchange) and authenticate each other in a simple way using identity-based cryptography. We indicated that security analysis of an identity-based authentication protocol. Our solution also presents key agreement between two users in cloud data storage. They also can authenticate each other. It not only provides privacy and secrecy but is also more effective than other identity-based key management schemes. This aligns well with the idea of cloud data storage to allow users with average to outsource their computational tasks to more powerful servers.

REFERENCE

- [1] Rajasudhan, S., & Nallusamy, R. (2014). A Study on Cryptographic Methods in Cloud Storage. *International Journal of Communication and Computer Technologies*, Vol 02-No.01, Issue: 02 March 2014.
- [2] Xia, Y., Kuang, L., & Zhu, M. (2010). A hierarchical access control scheme in cloud using HHECC. *Information Technology Journal*, 9(8), 1598-1606.
- [3] Wu, R., Ahn, G. J., & Hu, H. (2012). Secure sharing of electronic health records in clouds. In *CollaborateCom* (pp. 711-718).
- [4] Wenjun Luo and Min Xu "Hierarchical Identity-based Key Management in Cloud Computing", *Journal of Convergence Information Technology*, doi : 10.4156/jcit.vol.7.issue20.41, Vol. 7, No. 20, pp. 343-350, 2012.
- [5] Schridde, C., Dornemann, T., Juhnke, E., Freisleben, B., & Smith, M. (2010, June). An identity-based security infrastructure for Cloud environments. In *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on* (pp. 644-649). IEEE.
- [6] Gentry, C., & Silverberg, A. (2002). Hierarchical ID-based cryptography. In *Advances in cryptology—ASIACRYPT 2002* (pp. 548-566). Springer Berlin Heidelberg.

- [7] He, H., Li, R., Dong, X., Zhang, Z., & Han, H. (2012). An efficient and secure cloud-based distributed simulation system. *Appl. Math*, 6(3), 729-736.
- [8] Yan, L., Rong, C., & Zhao, G. (2009). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In *Cloud Computing* (pp. 167-177). Springer Berlin Heidelberg.
- [9] Elbaz, H. A., Abd-elaziz, M. H., & Nazmy, T. (2014). Trusting Identity Based Authentication on Hybrid Cloud Computing. In *Cloud Computing* (pp. 179-188). Springer International Publishing.
- [10] Boneh, D., & Franklin, M. (2001, January). Identity-based encryption from the Weil pairing. In *Advances in Cryptology—CRYPTO 2001* (pp. 213-229). Springer Berlin Heidelberg.
- [11] Chaturvedi, S. K., Swami, D. K., & Singh, G. Efficient-IBE (Identity based Encryption) based Cloud Data Storage Security Technique for Multi-user Inspection System.
- [12] Parsha, S. K., & Pasha, M. K. (2012). Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption (HIBE). *International Journal of Scientific & Engineering Research*, 3(5), 1-5.
- [13] Kalaichelvi, R., & Arockiam, L. (2013). Secure and Robust Cloud Storage with Cryptography and Access Control. *International Journal of Computer Science and Engineering (Elixir)*, Issue, (56), 13481-13485.
- [14] Al-Sabri, H. M., & Al-Saleem, S. M. (2013). Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security. *International Journal of Computer Science Issues (IJCSI)*, 10(2).
- [15] CSA (Cloud Security Alliance), USA. Online: <http://www.cloudsecurityalliance.org/guidance/csaguide>. V3.0, (2011).
- [16] Patil, D. H., Bhavsar, R. R., & Thorve, A. S. (2012). Data security over cloud. *International Journal of Computer Applications*.
- [17] PENG, Y., ZHAO, W., XIE, F., DAI, Z. H., GAO, Y., & CHEN, D. Q. (2012). Secure cloud storage based on cryptographic techniques. *The Journal of China Universities of Posts and Telecommunications*, 19, 182-189.
- [18] Agme, V. S., & Lomte, A. C. (2014). Cloud Data Storage Security Enhancement Using Identity Based Encryption. *Identity*, 3(4).
- [19] Kaaniche, N., Boudguiga, A., & Laurent, M. ID-Based Cryptography for Secure Cloud Data Storage. In *2013 IEEE Sixth International Conference on Cloud Computing*.