Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security

Hamdan M. Al-Sabri, Saleh M. Al-Saleem

**Department of Information Systems, College of Computer and Information Sciences, King Saud University
Riyadh, Saudi Arabia**

Abstract

Cloud computing is one of the most important way that allow us to share distributed resources now a days. Also it is more complex in nature and results in many security-related issues. Overall data security is an important factor in cloud computing as encryption technologies play a key role in securing data in the cloud storage. Moreover the outsourcing of data storage is the main concern in terms of security. In order to ensure the confidentiality of date during transferring it to the cloud storage, we need some encryption techniques. This paper proposed Cloud Storage Encryption (CSE) Architecture by using encryption/ searchable encryption technologies to provide a high level of data protection during data transfer to cloud storage. The proposed Architecture is composed of seven components (Director generate Keys and privileges, Data Users, The role of users, Encryption Point, Decryption Point, Searchable Encryption , and Cloud Data Storage). The CSE Architecture allows to encrypt data and to index it in a manner that ensures the protection of data during transportation. Also it allows the search process in the form of encrypted data and the retrieval of data in a safe manner. Moreover, the policies of encryption / decryption and access methods are discussed.

Keyword: *Cloud Computing, Security, Encryption Techniques, Cloud Data Storage (CDS), Cloud Data Storage Security (CDSS), Cloud Storage Encryption (CSE) Architecture.*

1. Introduction

Cloud computing is a broad concept for the exploitation of the network infrastructure and the ability to share different sources online. Cloud computing is a term that describes a working platform and the type of application that produces specific services and servers in the cloud may be physically or in the form of virtual machine. One of the most important issue in cloud computing is the security of customer data that host in cloud computing storage [1, 2]. Also the Security of data in cloud is one of the most important challenge and needs to be the main concern in cloud technology [9, 10].

The main challenge in cloud computing is the level of security of sensitive data that was stored using the cloud. Security in cloud computing is not a new issue and even one of the most complex problem. Based on the importance of security in cloud computing, it has become more important and grow tremendously as a result of the evolution of networking technology, scalability, and implementation of modern technologies [5]. Data storage system in the cloud must provide the necessary security requirements for user's data, including reliability, performance, availability, data consistency, distribution, confidentiality through the use of any modern techniques [6]. There are many cloud service providers such as google, IBM, Amazon, Sun Micro, and Microsoft. Also there are many cloud data storage (CDS) providers such as Sun, HDF, CloudNAS, and GFS. Many cloud service providers working to protect the stored data, but without integration between authorization and encryption that makes cloud data storage very secure, it is impossible. For that, to solve the problem of confidentiality in the cloud we can enforce encryption for certain types of data, as well as giving specific access privileges to data in cloud data storage. Since the data placed in the cloud can be accessed by any individual, as well as protection is

not guaranteed, we suggest in this paper the use of encryption technologies.

In this paper, we present the Architecture for enhancing the cloud storage security that is called (Cloud Storage Encryption (CSE)). CSE Architecture consists of seven components (Director generate Keys and privileges, Data Users, User roles, Encryption Point, Decryption Point, Searchable Encryption , and Cloud Data Storage). This Architecture is used to transfer the organization's Data or the average user in encrypted form to cloud storage. Subsequently help to data security, and eventually lead to the confidentiality of data during transportation, as well as during storage in the cloud storage.

The rest of this paper is organized as follows; Section 2 will present background and related work. In section 3, The Cloud Computing, Cloud Computing Architecture, Security Issues of Cloud Computing, Cloud Data Storage (CDS) will be explained; The Secure Storage, Cloud Data Storage Security (CDSS) , Retrieval of Encrypted Data in Cloud by Using (Searchable Encryption), and motivation will be presented in sections 4 and 5. The proposed Architecture for Cloud Storage Encryption (CSE) and Policy encryption / decryption and access methods will be explained in section 6, and finally we will draw the conclusion and future research work.

2. Background and Related Work

Cloud computing result from the interaction between grid computing and utility computing as it tend towards the distribution of IT resources such as storage, applications, business, services[22]. Since cloud computing moving towards expansion in all sectors, concerns growing in terms of security, as the effectiveness and efficiency mechanisms and methods of security in cloud computing are starting focus heavily. Cloud storage is a model for online storage and using networks where data is stored in the virtual stores [19].Encryption technology is one of the reliable technique to solve the problem of security and privacy in a cloud environment, As many types of encryption techniques are adopted as a solution to secure cloud computing and mainly focused on the security storage [24, 25], as well as secure computing and using the services [26, 27]. Basic requirements for cloud storage systems include large data warehouses and low-cost capacity, but users are reluctant to transfer sensitive and important data to the cloud because of security and privacy issues. To deal with these issues of security and privacy in cloud storage many cloud storage architectures are proposed that are mostly based on encryption [29, 30].

In paper [3] the authors presented and evaluated eight modern encryption techniques (RC4, Rc6, MAR,..) for independent platform and used NIST statistical testing. Paper [6] explained a literature review of the concepts and the theoretical aspects of security frameworks as explained MAC that was implemented in cloud. Another approach presents idea about some areas that could use the encryption and are quickly adapted to cloud computing [7]. [16] In another paper, they proposed a way to build reliable cloud computing environment through the use of encryption/ decryption methods, and compression. In [19] the authors presented a cipher text policy attribute-based encryption (CP-ABE) as encryption solution to enable the owners of the data from the definition of their own access property and access policy. Paper [23] they have contributed to give a summary of the results of search for security storage in the cloud that uses encryption technologies during design. Cloud Storage Encryption (CSE) architecture was proposed. The architecture supports security storage in cloud computing by using encryption/ searchable encryption techniques to protect Data during transportation and storage in the cloud and also to enable the search in encrypted data easy and confidential.

3. Cloud Computing

The simplified definition for Cloud Computing is to move computing from the PC to a central data over the Internet. Also, Cloud Computing is isolated a lot of complexity that associated with cost, components management, and software and make it easy service via the Internet. As the cloud computing consists of modern technological concepts such as Service Oriented Architecture (SOA), Web Services (WS), and communication infrastructure. Cloud computing has five characteristics that distinguish them from the rest of the systems based on the Internet [3, 16, 18, 23]:

- *Resource sharing*: Cloud computing depends on business where the different

users can share resources and use the same resources in the same level of network,

- *Scalability*: Cloud computing has the flexibility to expand in terms of users or storage,
- *Flexibility*: Cloud computing provides users flexibility in terms of increasing or decreasing the resources used,
- *Pay as you used*: In cloud computing cost is calculated based on its use, and
- *Self-identify resources*: In cloud computing subscribers can determine the appropriate capacity for them related to processing, software, and storage.

There is also a set of characteristics of *Cloud Computing Service* that distinguish them from traditional computing e.g. a self-service application, the broad scope of access across the network, the pooling of resources, collaboration between many users, flexibility, anywhere/ any time access and the possibility of rapid measurement services [4,16]. As the growing popularity of cloud computing calls attention to data processing in the cloud, there are benefits of storage in the cloud Such as access from anywhere, flexibility, scalability, cost-effectiveness, but the main problem is the security of the data that has been stored [7].

3.1 Cloud Computing Architecture

Cloud computing in general that it works to promote scalability, homogeneity, flexibility, low cost, geographical distribution, service-oriented and advanced security technology, but through the above we can classify Computing architecture according to the type of cloud service types to [8, 16, 23] as shown in figure1:

Cloud Service Delivery Models: Divided into three main categories:

a. *Cloud Software as a Service (SaaS):* The ability to provide applications to consumer on the infrastructure of the cloud, and consumer can also access applications through interfaces assigned to the customer, as the customer does not manage and control any infrastructure components of the cloud (such as the network, servers, computer systems, storage, applications).

b. *Cloud Platform as Service (PaaS)*: the ability to provide consumer with a property of distribution infrastructure for the cloud, such as create applications using programming languages and tools supported by the service provider, as well as the consumer does not manage or control the infrastructure.

c. *Cloud Infrastructure as a Service (IaaS)*: The ability to provide the consumer with the provision of treatment, network, storage, the main resources of computing, where the consumer has the ability to deploy the software.

Cloud Deployment Models: According to the three types mentioned above, there are four models for deployment of cloud services:

a. *Public Cloud*: cloud Infrastructure is available to the group of organizations.

b. *Private Cloud*: Cloud infrastructure available to a single organization.

c. *Community Cloud*: Cloud infrastructures shared between many organizations and share a set of characteristics in the cloud.

d. *Hybrid Cloud*: Cloud infrastructure consists of two clouds or more mentioned above.

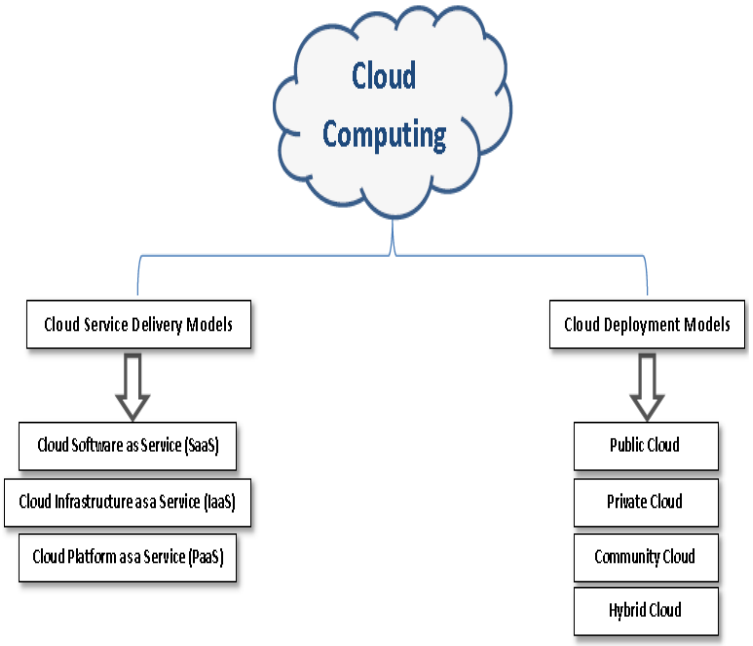

Figure 1. Cloud Computing Classification

3.2 Security Issues of Cloud Computing

Security and privacy risks is an important issue when the user wants the implementation of cloud computing and the use of cloud storage, Although the features and benefits of cloud computing-related cost, flexibility and ease of use, but there are many concerns related to security issues that need to be addressed as shown in figure 2, for example safe applications and sensitive data because it is in a shared environment. So you must develop a mechanism that provides integrated control to produce a high level of security.

Because the protection is not provided by the cloud, most companies are using their own security infrastructure [17]. It's important to know that cloud storage is a part of the *Cloud Infrastructure as a Service (IaaS)* in cloud computing [28]. To protect data in the cloud computing and when you use the cloud storage, the standard method is use encryption techniques to encrypted sensitive data [31], such as hemimorphic encryption, attribute-based encryption, searchable encryption, and broadcast encryption [32,33].

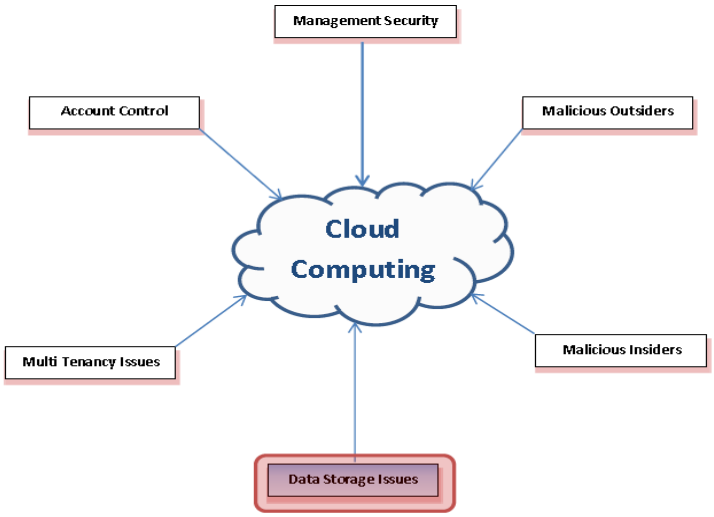

Figure 2. Cloud Computing Threats with more focus on Data Storage Issues

3.3 Cloud Data Storage (CDS)

Cloud data storage consists of a huge number of storage devices that distributed throughout the network; it also provides users with the normal structure of the cloud data storage, which include distributed file system, resource pool, service interfaces and service level agreements (SLAs), etc. [6]. CAS [28], Gave a definition of cloud storage is a branch of *Cloud Infrastructure as a Service (IaaS)* in cloud computing and it is working to provide the data, and reduce infrastructure costs by storing data remotely. Cloud data storage works to provide storage service for different levels of customers as the cost of storage depends on the space required the ability and bandwidth. To manage the contents of the data stored in the cloud data storage can rely on Service Oriented Architecture (SOA), Web Service (WS). There is a complementary and interoperability relationship between Cloud Data Storage (CDS) and Cloud Data Storage Security (CDSS) in order to make data in the warehouse more secure.

Cloud storage can be divided into two parts [23]:

- Cloud storage that is designed using encryption technologies and has no theoretical framework for encryption such as Kamara et al.'s scheme, Barua et al.'s scheme, Kumbhare et al.'s scheme , and
- Cloud storage that is designed using encryption techniques and it has theoretical framework for encryption such as Kamara et al.'s schema, Chow et al.'s work.

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 encryption techniques as shown in figure3.

4. Secure Storage

Secure Storage means to protect data from unauthorized access. From literature review on the secure storage always the risk is come from inside or the threat from outside [10, 11, 12]. In fact, Main risks that make companies do not tend to cloud computing is the secure storage of data. The main concept for secure storage in the cloud computing is to encrypt data in a reliable environment before being sent out of the cloud in an environment that is unreliable. There are as many encryption/ decryption techniques that work to protect data during transfer

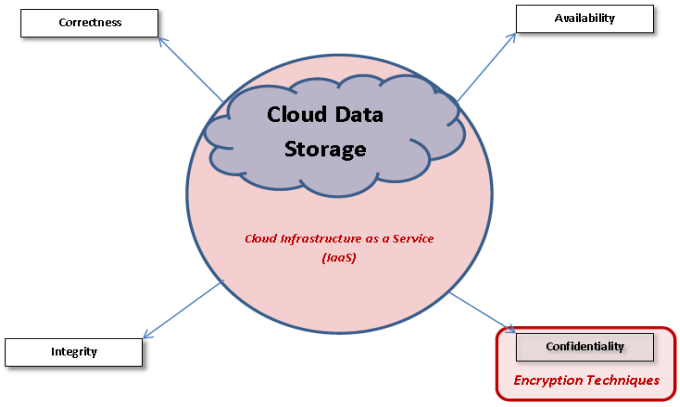

Figure 3. Security policies for cloud computing with a focus on Confidentiality

such as (AES, Blowfish, Serpent, etc.). The encryption for data used to ensures confidentiality of the data stored in the cloud computing. Most primitive traditional encryption technology proposed for data protection cannot be adopted directly [20, 21].

4.1 Cloud Data Storage Security (CDSS)

Cloud Data Storage Security (CDSS) include safe storage media that contains data security mechanism such as audit, authority, certificate, encryption, etc. As Cloud Data Storage Security (CDSS) applied on all storage procedures which include software, hardware, data, information, network security, and client's privacy security.

4.2 Retrieval Encrypted Data in Cloud by Using (Searchable Encryption)

Interesting problem related to encrypt data is the process of querying the encrypted data and retrieval [13, 14]. Searchable Encryption is a broad concept to handle and search in encrypted data. As the main objective of using this technique (Searchable Encryption) is a request encrypted data stored in external places and query and retrieve data without the need for decoding. The first searchable encryption schema was presented in 2000 by [15], and they used symmetric encryption. As there are many searchable encryptions schema using asymmetric encryption and public key for encryption such as public key encryption with key word search (PEKS).

5. Motivation to develop Cloud Storage Encryption (CSE) Architecture

Due to the prevalence of cloud computing and increase the use of cloud storage for storing sensitive and important data for companies; it has become necessary to find security architectural during the transfer of data to the cloud. This is done through the use of data encryption technologies; indexing, split, and distribution data between servers in the cloud to ensure data security, confidentiality and to find the appropriate way to retrieve encrypted data securely and in decrypted form. For all the reasons mentioned previously been proposed Cloud Storage Encryption (CSE) Architecture and the focus on Cloud Infrastructure as a Service (IaaS) because that cloud storage is located within this range and it has a special security requirements and general threats as explained in in Table 1 .

Table 1. Security Requirements for (IaaS) level in Cloud Computing

level	Service Level	Security requirements	Threats
Virtual level	Infrastructure as a Service (IaaS)	- Data Security(data transit, data at rest) - Virtual Cloud Security - Communication Security	- Data Modification - Data hijacking - Data interruption

6. The proposed Architecture

The main objective from Cloud Storage Encryption (CSE) Architecture is maintaining the security and confidentiality of the data during the transfer to cloud storage. As Cloud Storage Encryption (CSE) Architecture also allows to using encryption techniques during the transfer of data to cloud storage, as well as research in the encrypted data and retrieval in a secret and fast way. Cloud Storage Encryption (CSE) Architecture consists of seven components (Director generate Keys and privileges, Data Users, User roles, Encryption Point, Decryption Point, Searchable Encryption , and Cloud Data Storage) as shown in figure 4.

1. *Director generate Keys and privileges*: A center within the organization with a high level to generate public and private keys for data users and their roles within the organization, as well as granting special privileges to the suitable roles inside the organization,
2. *Data users*: Is a client or employee within the organization who owns the data and being a set of processes and sends it to the cloud storage,
3. *User Roles*: This aspect determines the characteristics and privileges for user by depending on sections, for example, the Finance Department, or the Procurement Section etc. and through which the inclusion of specific code during transfer the data depending on the type of partition,
4. *Encryption Point*: At this point is determine what type of data users and roles by codes and then indexing data, encryption indexed data, divided data into several packages where each package is stored in a different server and inclusion of a specific code in divided packets so can be assembled during the retrieval,
5. *Searchable Encryption*: A special techniques to search in encrypted data during the retrieval of data from cloud storage without the need for decryption as it works to hide the query and control of the search process and compile

divided packages and then delete the query to save the confidentiality of the retrieved data from the cloud storage,

6. *Decryption Point*: Through which to decode encrypted retrieved data using private keys that have been granted to users based on their roles and thus ensure the confidentiality of data during its transfer to the trusted environment, and
7. *Cloud Data Storage*: An entities and private databases for data storage and post service allows sharing data during storage,

6.1 Policy encryption / decryption and access method

One policies task during encryption will determine the structure of private keys that have been defined by the key generators. After that the package that will be encrypted and inclusion code of specific properties keys by type of user and their roles and then the encrypted data is indexed and divided into packages to be distributed between servers. User will be able to search the encrypted data through the use of searchable encryption technology and using the private key to decrypt encrypted retrieved data and to assemble packages that were distributed between servers using own code and that policy is guaranteed to safe and confidential data.

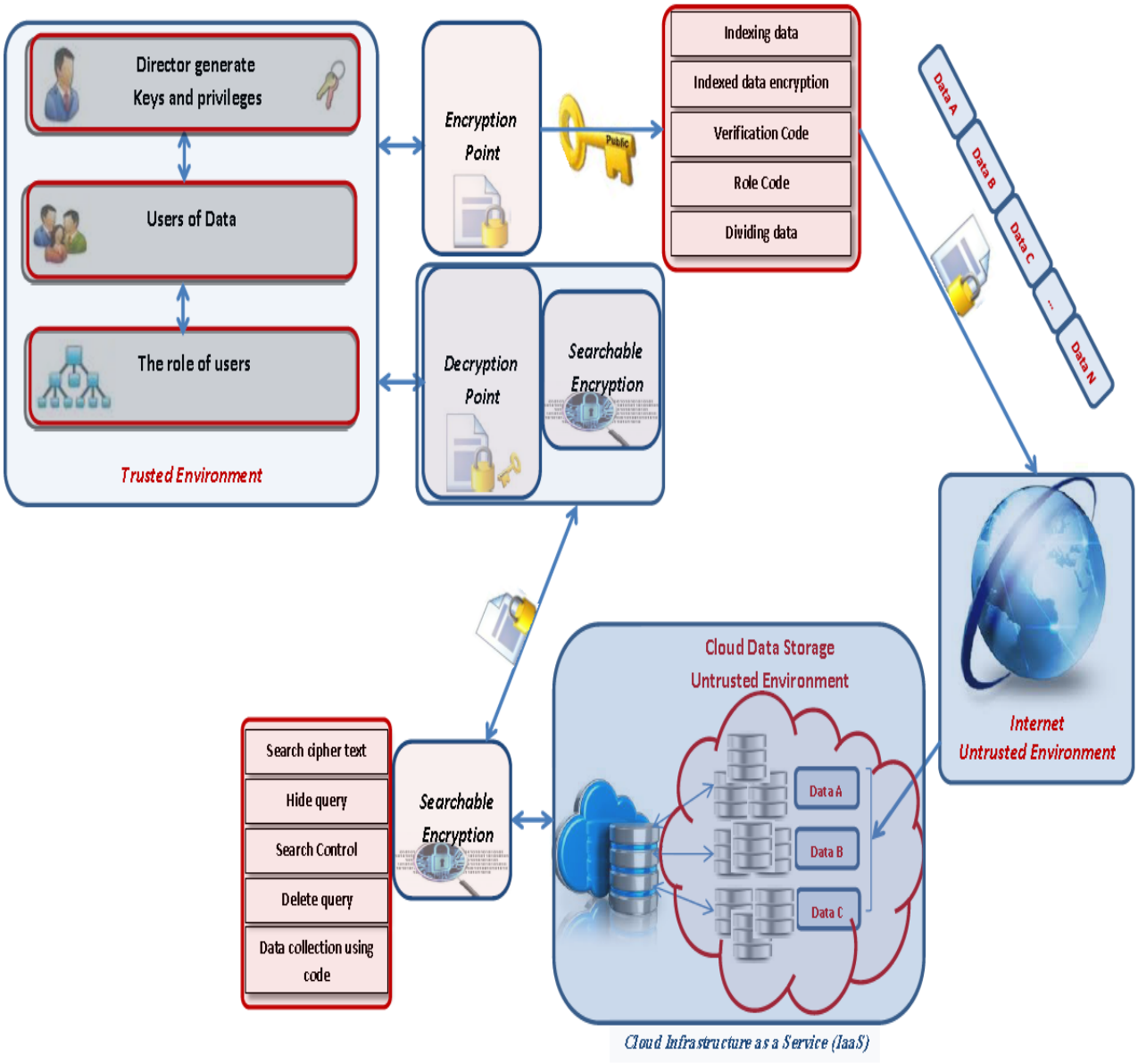

Figure 4. Proposed Cloud Storage Encryption (CSE) Architecture

7. Conclusions and further work

In this paper, a new architecture that handles data transfer securely to cloud storage has been proposed. The Cloud Storage Encryption (CSE) Architecture and Policy encryption / decryption and access method have been identified in order to show how data can be transfer to cloud computing storage environment. The integrated work flow between encryption point, decryption point and searchable encryption has been presented as CSE Architectural components and interaction between components is explained. We are planning to use the quality of services (QoS) to test the performance of all components with the CSE Architecture as our future work. Also, we plan to apply how to separately control the cloud data storage security and the rules of generating keys from the separate view.

References

[1] Luis M. Vaquero1, Luis Rodero-Merino1 , Juan Caceres1, Maik Lindner2 "A Break in the Clouds: Towards a Cloud Definition ", ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, 2009.

[2] John W. Rittinghouse James F. Ransome "Cloud Computing Implementation, Management, and Security".

[3] Sherif El-etriby, Eman M. Mohamed " Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing ", ICCIT, 2012.

[4] John W. Rittinghouse James F. Ransome "Cloud Computing Implementation, Management, and Security".

[5] Anderson R. (2001). In: Security engineering: a guide to building dependable distributed systems. New York: John Wiley & Sons Inc; 2001.

[6] Amir Mohamed Talib," Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature Review", Computer and Information Science, Vol. 3, No. 4; November 2010.

[7] Isaac Agudo, David Nuñez, etc, " Cryptography goes to the Cloud".

[8]Cloud Security Alliance www.cloudsecurityalliance.org http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf /.

[9] Yanpei Chen, Vern Paxson and Randy H. Katz, "What's New About Cloud Computing Security?" Technical Report No. UCB/EECS-2010-5, http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html, Jan. 20, 2010.

[10] RSA, The Role of Security in Trustworthy Cloud Computing.

[11] Ebenezer A. Oladimeji, Security threat Modeling and Analysis: A goal-oriented approach, 2006.

[12] Ristenpart, Thomas and Tromer, Eran and Shacham, Hovav and Savage, Stefan, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, 2009.

[13] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. 1998. Private information retrieval. J. ACM 45, November 1998.

[14] Kushilevitz, E.; Ostrovsky, R. , "Replication is not needed: single database, computationally-private information retrieval," Foundations of Computer Science, 1997.

[15] Song, D.X., Wagner, D., Perrig, A.: Practical techniques for searches on encrypted data. In: 21st Symp. On Security and Privacy (S&P), Berkeley, California, May 2000, pp. 44–55. IEEE Computer Society, Los Alamitos, 2000.

[16] S.Sajithabanu, Dr.E.George Prakash Raj, " Data Storage Security in Cloud ", IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011.

[17] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, 2010.

[18] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[19] B. Raja Sekhar,B. Sunil Kumar, L. Swathi Reddy, V. PoornaChandar, "CP-ABE Based Encryption for Secured Cloud Storage Access", International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September-2012.

[20] Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. PKC 2011.

[21] Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (Hierarchical) inner product encryption. EUROCRYPT 2010.

[22] Sahai, A., Waters, B.: Fuzzy identity-based encryption. EUROCRYPT 2005.

[23] PENG Yong1, ZHAO Wei, etc. "Secure cloud storage based on cryptographic techniques", ScienceDirect, October 2012.

[24] Bessani A, Correia M, Quaresma B, et al. DEPSKY: dependable and secure storage in a cloud-of-clouds. 6th Conference on Computer Systems
(EuroSys'11), 2011.

[25] Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data. IEEE 30th International Conference on Distributed Computing
Systems (ICDCS), 2010.

[26] Danezis G, Livshits B. Towards ensuring client-side computational integrity. 3rd ACM Workshop on Cloud Computing Security Workshop (CCSW'11),
New York, ACM. 2011.

[27] Takahashi T, Blanc G, Kadobayashi Y, et al. Enabling secure multitenancy in cloud computing: challenges and approachs. 2012 2nd Baltic Congress on Future Internet Communications (BCFIC), 2012.

[28] Cloud security alliance. Security Guideline for Critical Areas of Focus in Cloud Computing V3.0, 2011.

[29] Kamara S, Lauter K. Cryptographic cloud storage. 14th International Conference on Financial Cryptography and Data Security, LNCS, IFCA/Springer-Verlag. 2010.
[30] Popa R A, Lorch J R, Molnar D, et al. Enabling security in cloud storage SLAs with Cloud Proof. Microsoft TechReport MSR-TR-2010, 2010.
[31] Tang Y, Lee P P C, Lui J C S, et al. FADE: secure overlay cloud storage with file assured deletion. Security and Privacy in Communication
Networks. 2010.
[32]Chase M, Kamara S. Structured encryption and controlled disclosure. ASIACRYPT 2010, LNCS. 2010.
[33] Liu Q, Tan C C, Wu J, et al. Reliable re-encryption in unreliable clouds. IEEE Global Telecommunications Conference (GLOBECOM), 2011.

Hamdan M. Al-Sabri received his B.Sc. degree in computer science in 2009 and his Master degree from King Saud University in 2011, and he is currently doing his PhD at the department of information Systems, college of computer and information sciences, King Saud University, Saudi Arabia. Al-Sabri has published papers in SOA, Knowledge Management, ERP, and Computer Security.

Saleh M. Al-Saleem Dr. Saleh Al-Saleem , Associate Professor in College of Computer and Information Science, King Saud University. He received his PhD from Wayne State University, Michigan, USA, 2001, in the field of computer science (Evolutionary Computation). He received his Master degree in computer science from Ball State University, IN, USA 1996, and His BS degree in computer science from College of education, King Saud University, Saudi Arabia 1991. He served as the dean of admission & registration in Shaqra University, and also served as the head of IT and e-Learning in Shaqra University. Previously he worked as head of Information Technology department at the Arab Open University, and before that he worked as the head of Computer Technology department and faculty member in Riyadh College of Technology. Dr. Al-Saleem current research interests includes: evolutionary computation, Text Classification, ERP, BPM, e-Learning, and Open Source.