Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 11 (2013) 1202 – 1210

Procedia Technology

The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)

Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud

Hossein Rahmani*, Elankovan Sundararajan, Zulkarnain Md. Ali, Abdullah Mohd Zin

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Abstract

In recent years, there has been a vast interest in optimal usage of computing resources so that massive data can be processed with minimal cost. The need to use a pool of shared resources in a wide area network that provide elasticity, high capacity of computation and ability to store information on location-independent storages have led to the advent of cloud-computing. However, the global nature of cloud brings about some challenges in security domain when physical control over our information in cloud is impossible. Thus, encrypting critical data becomes essential, and strongly advisable. The server-side encryption in an untrustworthy environment like public cloud is too risky. On the other hand, client-side encryption can undermine the benefits of cloud since it is a time-consuming task for encryption and decryption. To address this issue, we developed a private cloud as an intermediary. In this paper, based on XaaS concept, we design an Encryption as a Service in order to get rid of the security risks of cloud provider's encryption and the inefficiency of client-side encryption.

Selection and peer-review under responsibility of the Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia.

Keyword: Cloud computing; Cryptography; EaaS; Parallell Processing; Security

1. Introduction

Nowadays, the vast increase of volume of data as a result of advent of internet and electronic information, has forced the enterprises to deal with sudden changes in the type and number of their processing systems. They should make a significant afford to keep their hardware and software up to date while the information technology drives a

* Corresponding author. Tel.: +60-147-015_410
E-mail address: hnrahmani @yahoo.com

Selection and peer-review under responsibility of the Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia.
doi:10.1016/j.protcy.2013.12.314

rapid and non-stop train towards innovation. Therefore, in the dilemma, it seems to be rational to use a more dynamic computing model like cloud-computing that provides updated resources as a service on a demand and a fraction of the cost just by paying as you use. Rapid elasticity and flexibility have made it extremely interesting to the public and for specific sectors like health care and insurance companies. Cloud along with web-based applications have revolutionized the current life so that we can interact with each other via web-based products and the cloud offered by vendors such as MSN, Yahoo, Google, Amazon, etc. On the other hand, in spite of the mentioned tendency to migrate to cloud; some facets in cloud bring about some barriers for enterprises. The concerns about cloud are categorized in two main categories: business issues and technological issues [1]. Among those issues, security has always been a major concern in Open System Architectures. Since in cloud-computing, program and customer data are residing in cloud provider's location, more serious concerns can be observed in security. Generally, we should keep data safe from some dangers such as disruptive services, damaging information, stealing information and loss of privacy as well as some vulnerability such as corrupting communication or eavesdropping and hostile programs.

In cloud where we do not have desired physical control over our data, cryptography seems to be the best way for protecting sensitive information. It helps to guard against data loss and theft. In fact, encryption is used for data confidentiality and integrity. Characteristic of multi-tenancy and easy provider's access to data force us to provide data confidentiality through the combination of contractual liability, access control and especially encryption.

Although cryptography is the best solution to keep the sensitive data on the servers of cloud, there are some problems when client-side encryption can undermine the advantages of cloud since it is the time-consuming task. Moreover, it is not safe when all certificates and keys save on a client while flexibility in cloud allows to be connected to cloud through other desktops or PDAs. Furthermore, in case of forgetting key, user will lose his data on cloud. On the other hand, server-side encryption in a public environment has disadvantages because of multi-tenancy characteristics, unsatisfied malicious, dismissed employees or even outside attackers that can increase the probability of fraud, collusion and falsified transaction. In this paper, we will show that EaaS, by unifying control and management of cryptography can eliminate the problems of client and server side encryption while reduces operational costs.

2. Related Works

In an unreliable environment like a public cloud, storage and computation have to be secure enough. In this section, in order to make a cloud secure and trustable, some kinds of cryptographic techniques deployed in cloud-computing are discussed. In addition to traditional physical security, authentication and authorization methods, we enjoy some customized cryptographic techniques such as identity-based encryption, attribute-based encryption, homomorphic and searchable encryption, isolation of encryption/decryption, combination of symmetric and asymmetric algorithms.

2.1. Identity-based encryption

Shamir introduced utilizing identity of user in which a user's identity like email address was replaced by a digital certificate [2]. In [3], Barua used identity-based encryption for making safe communication in a personal health environment in which the information should be stored in the cloud. The suggested scheme is based on two major phases. The goal in the first phase is safe communication between existing entities such as user, service provider, Data requesters (doctors, general users and pharmacists) and cloud storage. For achieving this purpose, after some initializations by the service provider, the user will encrypt the data by public key and receiver's identity. Then, verification on data originality is done by using digital signature in the receiver-side in order to gain data integrity.

Second phase emphasizes on proper data access for requesters. Since the patient does not know which requester is in health care system, access control should be provided by the scheme remotely on attribute-based policy. The authors created an access tree based on different roles and privacy level of the requesters and assigning attribute set to each of requesters to solve the problem. In this scenario, data requester is not able to learn unnecessary attributes.

2.2. Attribute-based encryption

In the sphere of trustworthy computing, the attribute-based encryption (ABE) has emerged for access control based on role-based characteristics. In such a scheme, the ciphertext will be associated with a formula so called access formula, while secret key will be linked to some attributes. If these attributes satisfy access formula, the scheme will permit to decrypt the ciphertext and will achieve plaintext. This idea was first raised by Sahai & Waters [4].

In cloud-computing where encrypted data are traditionally stored on servers, we have to reveal the secret keys for authorized users. This needs an efficient mechanism to manage and distribute keys. Also, in the case of a large number of authorized users, or revocation of authorized user's responsibility, efficiency will be destroyed. Thus, Wan enhanced CP-ASBE (Ciphertext Policy Attribute Set Based Encryption) scheme which proposed by Bobba [5] just by adding a hierarchical structure that provides more scalability and flexibility. The notion utilizes a delegation algorithm for enhancement. In a hierarchical structure as it has been indicated in Figure 1, the trusted authority party manages master keys distribution and domain authorities and they in turn administer the owners or consumers of data for data encryption/decryption and key delegation in their sub-domain. These domain authorities are just trustable in their domains. Data are also stored on the storage of cloud provider. In spite of CP-ASBE, owners/consumers delegate their tasks to the mentioned authority parties and the cloud provider so that owners/consumers can be online just in the necessary time. The security of the scheme is equivalent to security rate in CP-ABE [6].

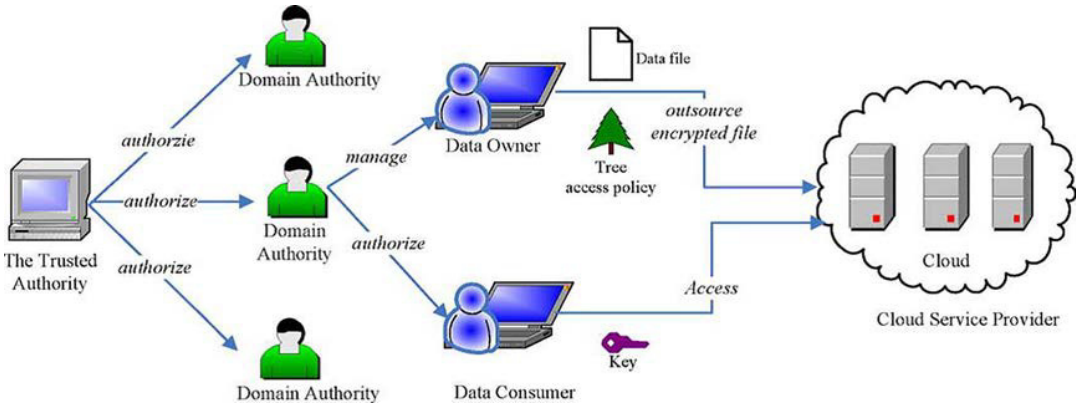

Fig 1. Hierarchical system model in HSABE scheme

2.3. Homomorphic and searchable encryption

With the advent of cloud-computing and the necessity of third party for data storage and data process, probability of malignant acts or collusion has increased. Thus, researchers have stressed on modality of encryption in such unreliable environments. Searchable encryption or homomorphic encryption is an efficient technique for coping with such an unreliable environment by searching or doing the operation on encrypted data with no need to decryption.

Boneh suggested a model of encryption that supports searching based on keyword (PEKS). For example, he intended to check a keyword in an encrypted email by the receiver's email gateway without decryption and just by utilizing a trapdoor provided by receiver [7].

Work of Gentry, [8], can be considered as a revolution in homomorphic encryption scheme in which ciphertext is derived from multiplication of key and a random number q plus plaintext, $c = p*q + m$. This is a kind of fully

homomorphic function by considering *m* as the residue *c* modulus *p*.

Hou proposed a scheme for investigating data so that investigators can access to their demanded data by preserving privacy for other users when the service provider is even unreliable. This scheme is divided into two phases: in the first phase authors employ homomorphic encryption in order to search on encrypted data by the administrator and investigators' encrypted keywords. In this phase, it is supposed that the administrator is a trustable person who returns all demanded results. Of course, he/she is not able to know about keyword and data because he/she does not have private key for decrypting. In the second phase, they revoked the primary assumption about administrator and delegated the supervision on the administrator to the trusted third party. This task is done by utilizing commutative encryption in which $Ep_A(Ep_I(m)) = Ep_I(Ep_A(m))$. Ep_A is encryption by the administrator's public key and Ep_I is encryption by the investigator's public key [9].

Finally, Sutar & Patil proposed a framework in cloud-computing by considering three parties including third party, cloud user and cloud server. Then, they categorized personal information into three categories such as personally identifiable information (*m1*), sensitive information like password (*m2*) and general information like registration number (*m3*). Finally, by using homomorphic encryption, a mechanism was proposed to exchange this information among the mentioned-parties, so that anonymous privacy can be achieved. In this work, authentication process was done by a third party after comparing credentials from cloud user and cloud server. Therefore, this scheme decreased server computation while it preserved user's information from third party and attacker. In this work, authors assumed that the cloud server is safe enough to save user's information; meanwhile solution has been only suggested for authentication rather than for a data processing on multi-user scheme [10].

2.4. Isolation of encryption/decryption

This category of research addresses the problem where encrypted data and decryption key have to be stored in storage on public cloud that is naturally unreliable due to the possibility of being abused by malicious insiders. One solution to this problem can be complied by authority division that is common in business management in which, for instance, a cashier has a different responsibility of an accountant or stamping official documents by two various seals in order to avoid of any abuse.

Hwang proposed such a business model in the cloud so that encryption and decryption are separated from storage function [11]. For example, user runs a login program for user verification. Then, when CRM program distinguishes him as an authorized user, this request along with user ID is sent to storage cloud. After finding corresponding encrypted data, data and user ID are transmitted to Encryption & Decryption service to decrypt. Theses decrypted data through a secure channel with CRM will be accessible for user. Then, Encryption and Decryption service (EDS) will remove the whole data related to the process.

2.5. Combination of symmetric and asymmetric algorithms

Cunsolo proposed a solution based on the combination of symmetric algorithms with better performance and asymmetric algorithms with more security. In the proposed solution, data should be encrypted by a symmetric algorithm while the corresponding key can be encrypted by utilizing an asymmetric one. Since asymmetric algorithms have the key pair for encrypting/decrypting functions, just owner of the private key can decrypt the symmetric key. Storing public key together with data, makes the availability to data and public key by the owner in each node of distributed network. In this work, it is supposed that the decryption process is done in the similar storage of the user's certificate in the user node [12].

Most of the above-mentioned techniques are just theoretical at this point. Thus, they need a long time to run that makes them impractical. The current feasible solution is to utilize a trusted third party that suggests cryptography as a service.

3. Methodology

In order to prepare a trustable third party in role of EaaS, we should carry out three steps: first, implementing private cloud; second, providing encryption algorithms; and, last, multi-threading features based on a number of VM cores.

3.1. Implementing private cloud

In order to have an EaaS, the first step is implementing private cloud. A private cloud allows the users to have more control over the infrastructure and security due to more restriction on the network and user access. Moreover, in a private-based cloud, the processed data within the organization are protected against legal issues and are not affected by network bandwidth's restrictions during processing time. However, they do not benefit from the large number of computing resources, as public cloud may offer; they are still large enough to enjoy the advantages of cloud-computing. Furthermore, in the private cloud, it is possible to apportion the users' workloads on different resources depending on enterprises' size [13].

From a different view, in a private cloud, there are a group of users that share the virtual instances, while they are monitored constantly in comparison with heterogeneous users in the public cloud. Furthermore, availability of services may be guaranteed in a private cloud, which has been designed for the specific purpose of the enterprise.

For implementing a private cloud, we need utilizing a framework for designing and implementing an IaaS (Infrastructure as a service). Some of the well-known frameworks for the purpose are OpenNebula, Nimbus, OpenStack and Eucalyptus.

In fact, the suitable framework depends on user and application requirements. OpenNebula is easy to install; however, other frameworks like Eucalyptus have been improved in the final version. Since OpenNebula has no caching system for images, it is too slow to deploy. Eucalyptus and OpenStack act almost perfect when the servers are handful, but for hundred of servers and VMs, the time and failure increase. Nimbus has no acceptable networking management. Also, it does not support VMware. Furthermore, Nimbus, similar to OpenStack, is often released less than four months, that can be considered as a disadvantage. Amazon web services are a de facto standard and one of the best current public cloud. Thus, compatibility with that is extremely essential to have a standard and a hybrid cloud, which our EaaS needs. Among them, OpenStack is not fully compatible with EC2 and S3. Moreover, OpenStack is still very difficult to learn with insufficient documents. These can be led to unpopularity, unless they will be solved in coming versions [14].

In [15], the authors conducted a comparison between OpenStack and Eucalyptus. They measured taken time to obtain the resources when an instance was launched and called it VM launch-time. In serial launch of VMs, OpenStack behaves drastically faster but in parallel launch of VMs when there were three, four or more VMs, Eucalyptus behaves faster than OpenStack as it is shown in Figure 2. This is partly because Eucalyptus does not resend the image for several instances and partly due to the policy of OpenStack's management system, which considers VM instances launching individually. Finally, regarding interface comparison, they claimed that Horizon in OpenStack is not as strong as Right Scale in Eucalyptus. For example, integration a private into the public cloud is allowed via the interface.

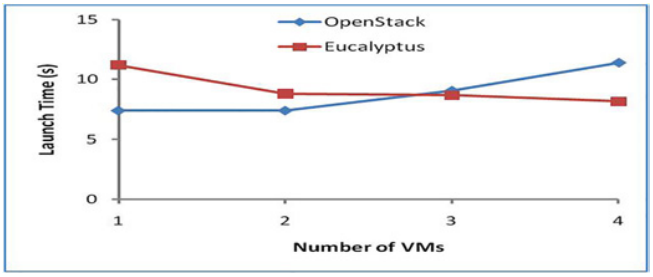

Fig 2 VM parallel launch time

Eucalyptus uses six components including node controller that is at the same machine with virtual machine instances and provides necessary resources, optional VB component in case of using VMware hypervisor, cluster and storage controller in cluster level of Eucalyptus and finally walrus and cloud controller for managing and querying other components. Due to improving inter-communication between Walrus and CLC as well as simplifying administration, also unnecessary requirement of high EBS volume in this work, we implement all components, except NC, inside a single physical machine as shown in Figure 3. Node Controller component together with necessary hypervisor is located on four machines. Finally, we use one laptop for managing the cloud components via EUCA2OOLS and dashboard.

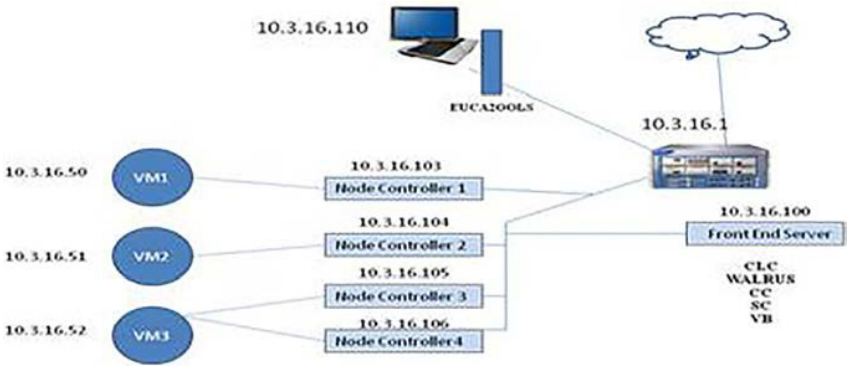

Fig 3. Sample private cloud configuration

3.2. Cryptography library

As we said before, the cryptography can address confidentiality and integrity. So, our EaaS scheme should provide semantic security against chosen plaintext attack as well as avoiding tampering, blocking and injecting of packets by adversaries. Since the confidentiality just provides security against eavesdropping, we have to utilize message authentication code (MAC) for having integrity. The only way to provide both confidentiality and integrity is using the authenticated encryption. The CryptoPP library by supporting a variety of algorithms and diversity of modes of encryption is a proper choice to use. For the combination of encryption and MAC, there are 3 strategies: if encryption is exerted at first as it is used in IPSec protocol, it is considered completely secure while simultaneous using on plaintext is insecure as it is utilized in SSH. The SSL protocol does encryption after authentication and can be secure in some constructions [16].

3.3. Multi-threading Model

In our scenario multi-users belong to a security group that can use similar or different algorithms. Moreover, each of them has several files that can be encrypted or decrypted. If the program is not written in a multi-threading level, it will not have the optimal performance on EaaS. In the former case, many of operations are done in a sequential process that will lose many resources, which are prepaid by our cloud. Accordingly, we need to do parallel processing in our program as well as our scheme.

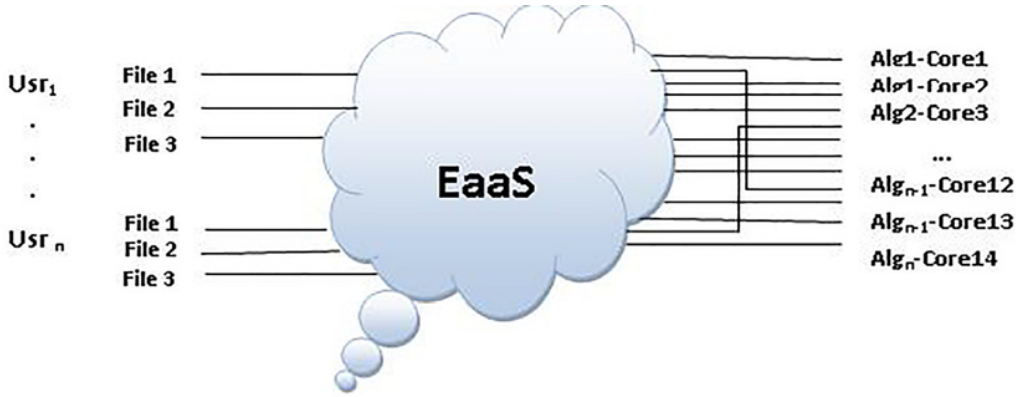

Fig 4. Multi-threading in EaaS

The simplicity, flexibility and portability make OpenMP as a proper library to implement parallelism. When a single thread hits the parallel region, it produces a team of threads. In the nested parallel region, each thread may create its own new team. The setting of the threads number depends on setting some Boolean properties in OpenMP library. Since we have some VMs with different cores, we determine scalable setting for the threads based on existing CPU cores in each VM. On the other hand, another important setting for parallelization is related to choose a suitable scheduling algorithm. Among four algorithms in scheduling process (static, dynamic, guided and runtime), guided algorithm makes less overhead on scheduling on different speed of processors or different work of any iteration in which the maximum of chunk-size and the remained iteration divided by the number of threads are considered for assigning to the next thread in each level.

4. Result and conclusion

In cloud computing where multi-tenancy, virtualization and outsourcing characteristics make it at risk of compromising security aspects and there is no physical control on data at rest or data in motion, the data can be protected by storing cryptographically and giving the key management to the authorized party. However, finding a trusted party for doing the important task in such an environment is very difficult. In order to solve the problem, the cryptography techniques need to be customized for the cloud environment. Some researchers with a combination of authentication and cryptography have tried to mitigate the abuse of any unreliable parties in the cloud. The identity-based authentication and attribute-based authentication are good examples of this category. Others tried to propose a model by encryption and decryption isolation from the storage service in the cloud. Another solution that emphasizes on the key management is deploying a combination of symmetric algorithms for data and asymmetric ones for keeping the keys. One of the best solutions that many of researches are involved in, is homomorphic encryption in which all functions are performed on the encrypted data. However, it is too slow in practice, and even no practical model has been seen for it. On the other hand, the client-side encryption, suggested by many researchers, mitigates the advantages of cloud.

So, the first problem in cloud-computing was lack of a trade-offs between client-side and server-side encryption. The server-side encryption provides a faster encryption and decryption by utilizing the resources of the cloud but in

an insecure third party. The client-side encryption provides almost more secure, but it undermines advantages of the cloud. Thus, it seems that implementing an in-house private cloud as a trusted party which offers encryption as a service can solve the problem. In figure 6, the time for six selected algorithms has been shown in the traditional client-side and the proposed EaaS. Single machine consists of i5-intel CPU with 3 GB RAM while our testbed in EaaS consists of a VM with 14 cores and 32 GB RAM. The tests were all performed on a 300 MB text file. The chart shows a considerable decrease in the time of encryption and decryption of the mentioned file. It illustrates that our EaaS performs more than six times better than a single computer in all algorithms. The utilizing of cloud resources and the deploying of multi-threading may be considered as the main reasons.

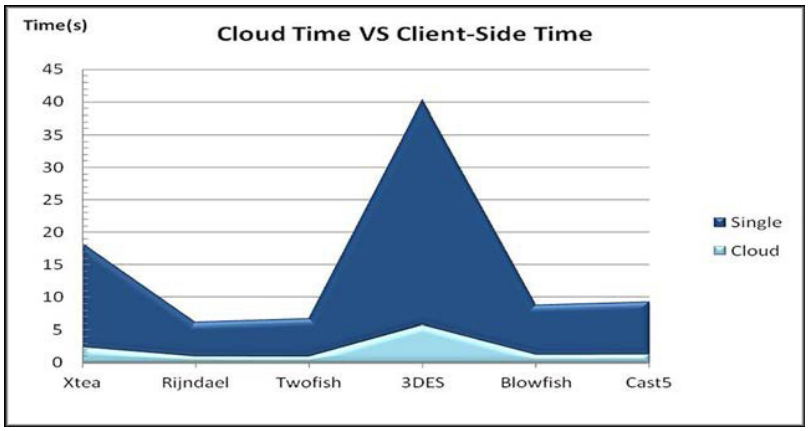

Fig 5. EaaS time versus client-side time

5. Future work

This work can be enhanced by comparison of well-known algorithms in different condition in order to find optimal algorithm in each case. Moreover, a general model can be proposed that include key management process. Furthermore, a model of authentication based on attribute or identity can be proposed for the EaaS. Finally, a fully homomorphic encryption algorithm can be modeled in this scheme.

6. Acknowledgements

We would like to express our deepest appreciation to the FRGS grant UKM-TT-02-FRGS 020502010 and DPP-2013-011grant for partially supporting this work.

References

[1] Yang H, Tate M. Where are we at with cloud computing?: a descriptive literature review.*ACIS 2009 Procedding*. 2009.
[2] Shamir A. Identity-based cryptosystems and signature schemes. *Advances in cryptology, Springer*;1985, p.47-53.
[3] Barua M, Liang X, Lu R, Shen X. ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing. *International Journal of Security and Networks*; 2011; 6(2), p.67-76.
[4] Sahai A, Waters B. Fuzzy identity-based encryption. *Advances in Cryptology–EUROCRYPT 2005*, p. 557.
[5] Bobba R, Khurana H, Prabhakaran M. Attribute-sets: A practically motivated enhancement to attribute-based encryption. *Computer Security–ESORICS 2009*, p.587-604.
[6] Wan Z, Liu J, Deng R. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. Information Forensics and Security, *IEEE; 2012;* 7(2), p.743-754.

[7] Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G. Public key encryption with keyword search. *Advances in Cryptology-Eurocrypt 2004, Springer*; 2004, p.506-522.
[8] Gentry C. Computing arbitrary functions of encrypted data. *Communications of the ACM*; 2010; 53(3), p.97-105.
[9] Hou S, Uehara T, Yiu S, Hui LCK, Chow K. Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), *Seventh International Conference on, IEEE*; 2011, p.378-383.
[10]Sutar S, Patil G. Privacy Management in Cloud by making use of Homomorphic Functions. *International Journal of Computer Applications; 2012;* 37(2), p.13-16.
[11] Hwang JJ, Chuang HK, Hsu YC, Wu CH. A business model for cloud computing based on a separate encryption and decryption service. *Information Science and Applications (ICISA)*, *International Conference on, IEEE*; 2011, p.1-7.
[12] Cunsolo VD, Distefano S, Puliafito A, Scarpa M. Achieving Information Security in Network Computing Systems. *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference*; 2009, p.71-77.
[13] Armbrus M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. *Commun. ACM*; 2010; 53(4), p.50-58.
[14] Laszewski G, Diaz J, Wang F, Fox GC. Comparison of multiple cloud frameworks. *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, IEEE*; 2012, p.734-741.
[15] Steinmetz D, Perrault BW, Nordeen R, Wilson J, Wang X. Cloud Computing Performance Benchmarking and Virtual Machine Launch Time. *Proceedings of the 13th annual conference on Information technology education, ACM*; 2012; p.89-90.
[16] Krawczyk H. The order of encryption and authentication for protecting communications (or: How secure is SSL?). *Advances in Cryptology—CRYPTO 2001, Springer*, p.310-331.