A Survey and Analysis of Security Models Used for On-Cloud Resources

Dr. Kamlendu Kumar Pandey
Assistant Professor, Dept of Information and Communication Technology
Veer Narmad South Gujarat University, Surat

Abstract—The sudden emergence of cloud as new computing platform has opened flood gates for host of diverse applications and services to be deployed on cloud. Most of the cloud service providers make claims to guarantee the performance and security to the deployed resources. However security is something which still haunts the developer for sole dependence on the providers. An effort has been done in this paper to understand the setup and models used for security services and what kind of benefits and assurances can be achieved from this. The models, architectures and frameworks are compared so as to increase awareness in the development community to ask relevant questions regarding security issues before deploying their applications.

Keywords — cloud computing, cloud security, information security, on-cloud applications, security models

I. INTRODUCTION

The term "Cloud Computing" [3] is about a complete system of deployment, operations and delivery of services to the clients universally and On Demand. It is about virtualizing hardware , software and logical resources on internet or intranet . Most of the cloud service providers provide a host of its own services, APIs and virtualized resources to the client. Apart from that they also allow clients to host clients services on their virtualized resources. This creates a win-win situation for both providers as well as clients. The provider generates a business model by charging for services while client is free from the burden of infrastructure for storage, running processes and software licensing. Although it seems to be good but it raises some valid alarms

1) Is my data which is stored on providers infrastructure is safe ?
2) Is the information which I transfer to and fro from provider and client remains confidential?
3) What arrangement has been made by the provider to make it confidential?
4) How do I guarantee the data leakage and theft from cloud?
5) How unauthorized access is handled by cloud?
6) What mechanism is used for message authentication
7) What are the legal aspects if privacy of resources is compromised
8) What about security of transactional data.
9) Is it using the modern refined security standards or the primitive one.

The above questions arise in the mind of cloud users which are not adequately answered by service providers. To understand the above question this paper describes various cloud security models and security used in the respective models. At the end there is comparison of various security schemes used for the cloud.

It is obvious that insufficient security services can render the cloud system non-trustworthy. For example, managing personal information or data of consumers in a public network requires a high degree of security [1-2]. In addition, there are some other aspects of cloud computing e.g., the movement of critical applications and sensitive data in cloud environment that need consistent care [4]. However, from the point of view of ease and cost of use the cloud computing is considerably
beneficial.

Indeed, the cloud computing requires to keep the data of every enterprise within the periphery of the enterprise. Further, emphasis is given on physical, logical, personnel security and access control specifications of the data [5]. Trust is also a major issue in cloud computing and it incorporates the fact that the confidence and assurance pertaining to people, data, object and information will execute or act in a projected way [10]. Moreover, in cloud computing data security, data integrity, and data leakage all are major issues and for all these issues cryptographic solutions are available. There are different algorithms to get the data security in

II. MODELS IN CLOUD COMPUTING

To analyze security in details one has to understand the various models being used in the cloud computing . The models are categorized on basis of deployment and delivery of services.[17-20] The are termed as

a) Deployment Model
b) Delivery Model

2.1 Deployment Model

The deployment models are based on the way the application and services are deployed and accessed on networks. The classifications are given as under.

a) Public Cloud: is a type of cloud hosting in which the cloud services are delivered over a network which is open for public usage. This model is a true representation of cloud hosting; in this the service provider renders services and infrastructure to various clients. The customers do not have any distinguishability and control over the location of the infrastructure. From the technical viewpoint, there may be slight or no difference between private and public clouds' structural design except in the level of security offered for various services given to the public cloud subscribers by the cloud hosting providers.

Public cloud is better suited for business requirements which require managing the load; host application that is SaaS-based and manage applications that many users consume. Due to the decreased capital overheads and operational cost this model is economical. The dealer may provide the service free or in the form of the license policy like pay per user. The cost is shared by all the users, so public cloud profits the customers more by achieving economies of scale. Public cloud facilities may be availed free an e.g. of a public cloud is Google.

b) Private Cloud: is also known as internal cloud; the platform for cloud computing is implemented on a cloud-based secure environment that is safeguarded by a firewall which is under the governance of the IT department that belongs to the particular corporate. Private cloud as it permits only the authorized users, gives the organisation greater and direct control over their data. What exactly constitutes a private cloud? It is difficult to define because when it's classified according to the services there are significant variations. Whether the physical computers are hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses that have dynamic or unforeseen needs, assignments which are mission critical, security alarms, management demands and uptime requirements are better suited to adopt private cloud. Obstacles with regards to security can be evaded in a private cloud, but in case of natural disaster and internal data theft the private cloud may be prone to vulnerabilities.

c) Hybrid Cloud: is a type of cloud computing, which is integrated. It can be an arrangement of two or more cloud servers, i.e. private, public or community cloud that is bound together but remain individual entities. Benefits of the multiple deployment models are available in a hybrid cloud hosting. A hybrid cloud can cross isolation and overcome boundaries by the provider; hence, it cannot be simply categorized into public, private or community cloud. It permits the user to increase the capacity or the capability by aggregation, assimilation or customization with another cloud package / service. In a hybrid cloud, the resources are managed and provided either in-house or by external providers. It is an adaptation among two platforms in which the workload exchanges between the private cloud and the public cloud as per the need and demand.
Resources that are non-critical like development and test workloads can be housed in the public cloud that belongs to a third-party provider. While the workloads that are critical or sensitive must be housed internally. Consider an e-commerce website, which is hosted on a private cloud that gives security and scalability, since security is not a prime concern for their brochure site it is hosted on a public cloud which is more economical as compared to a private cloud. Businesses that have more focus on security and demand for their unique presence can implement hybrid cloud as an effective business strategy. When facing demand spikes the additional resources that are required by a particular application can be accessed from the public cloud. This is termed as cloud bursting and is available with the hybrid cloud.
Organisations can use the hybrid cloud model for processing big data. On a private cloud, it can retain sales, business and various data and can initiate analytical queries over the public cloud as the public cloud is effective to meet the demand spikes. Hybrid cloud hosting is enabled with features like scalability, flexibility and security. If one is ready to overlook a few challenges like application program interface incompatibility, network connectivity issues and capital expenditures, then the hybrid cloud would be an appropriate option.

d) Community Cloud: is a type of cloud hosting in which the setup is mutually shared between many organizations that belong to a particular community, i.e. banks and trading firms. It is a multi-tenant setup that is shared among several organizations that belong to a specific group which has similar computing apprehensions. The community members generally share similar privacy, performance and security concerns. The main intention of these communities is to achieve their business related objectives. A community cloud may be internally managed or it can be managed by a third party provider. It can be hosted externally or internally. The cost is shared by the specific organizations within the community, hence, community cloud has cost saving capacity. A community cloud is appropriate for organizations and businesses that work on joint ventures,

tenders or research that needs a centralized cloud computing ability for managing, building and implementing similar projects.

2.2 Delivery Models

Delivery model of cloud computing are mainly of the three types. These are IaaS, PaaS, and SaaS.[19-21] Brief descriptions of these models are given below.

2.2.1 Infrastructure as a service (IaaS): Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.[6-9]

2.2.2 Platform as a service (PaaS): Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application .In PaaS, the user has an option of deploying the owned functional programs on the infra-structure of cloud [11]. PaaS is the service that offers the users to deploy user-designed or obtained applications on the cloud infrastructure [12]. In this cloud model, the cloud supplier provides a computing platform, logically comprising operating system, database, programming language implementation environment and web servers [13-16]. Further, in this model the web application and software (that use a wide range of programming languages and tools) developments are under the control of the user [22].

2.2.3 Software as a service (SaaS): The topmost layer of cloud computing delivery model stack is Software as a Service. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece software. A common example of a SaaS application is web-based chat where you can chat with your friends without having to manage feature additions to the chat product or maintaining the servers and operating systems that the email program is running on .SaaS is a software dissemination method which gives right to access the software and its functions tenuously as a web-based service [30]. In this service, the user can take benefit of all the applications. There is no need to install or maintain any additional software for using this service. According to some recent reports, SaaS is a rapidly rising market that predicts ongoing double digit growth [31]. This quick growth signifies that SaaS will become a humdrum within every organisation in near future. Perhaps it is important that buyers and consumers of technology must know what SaaS is and where it is suitable [30].

III. SECURITY ISSUES IN THE CLOUD COMPUTING MODELS

3.1 Security Issues in IaaS

The infrastructure as a service can have several loop hole of security which has to be looked upon. They can be listed as

a) Insecure APIs
b) Malacious Insiders
c) Shared Resources
d) Denial of Services
e) Stolen Credentials
f)

a) Insecure APIs

Most of the cloud providers provide a set of APIs to access their services. The APIs may have some vulnerabilities which can cause damage to the applications. The cloud provider is responsible for fixing these kinds of vulnerabilities, On the other hand, any update could change API settings, which may cause some customers' existing applications or functions to break. This could cause the provider to delay the release of some patches in order to give customers the chance to upgrade their software.

b) Malicious insiders

The whole system of IaaS is protected by a strong symmetric encryption to protect the sensitive data. These encryption strategies demand the storage of keys Depending on the cloud service's features; full encryption or the use of homomorphic encryption schemes may not be possible. If the private keys are stored on the cloud premises, then they are still in reach of a rogue employee of the cloud provider.

c) Shared resources

The cloud service providers normally share the hardware and virtualized resources with multiple clients. Hard disks, CPU, RAM, Cache Memories, and other elements were not typically designed with multiple privacy requirements in mind. There are chances of information leak in this case. Attacks side-channel timing attacks can happen which can leak cryptographic keys across virtual systems. Security weaknesses in components, such as the vitualizer, can lead to the compromise of the entire cloud infrastructure itself.. Cloud providers are constantly improving the isolation of resources in multitenant environments. The vulnerable hypervisors can be a serious concerns and may require an update after being improvised. This can create whole cloud to a shutdown and leave the clients stranded amount to huge financial and credibility loss.

d) Denial of service

This is an age old attack where the attacker exploit the systems by a continuous streams of request and thus using most of the resources. This situation can lead to deny the requests of other users. PING attack is a very common Denial Of Service Attack.. If attackers combine this with network-based denial-of-service (DoS) attacks, they could prevent customers from accessing their critical cloud resources. These attacks may even lead to an increased cost for the victim, as some providers bill the customer based on their use of resources. By now, all major cloud players have implemented mechanisms that make it very difficult for the performance of other users to be impacted on multitenant environments. Although cloud providers often do a better job of building their infrastructure with redundancy than many companies, it is still possible that some data could be lost forever. This could happen due to how errors are handled by the cloud provider, hardware failures, or an external attack.

3.2 Security Issues in PaaS

The platforms virtualized for the clients can range from Operating Systems, Web Servers, Application Servers, Mail Servers, JVMs, Frameworks etc. All such platforms may or may not be tested against code malfunctions,, memory leaks, virus or Trojan attacks. In PaaS, the application provider may facilitate the people to build applications on top of the platform. However, any security issue underneath the application level such as host and network invasion prevention will still be an anxiety for the application provider and the application provider has to provide strong assertions that the data rests inaccessible in-between the applications [23]. Consequently, it inclines to be more extensible than SaaS at the cost of customer-ready features. This arrangement outspreads the security features and proficiencies especially where the innate capabilities are less complete. However, this arrangement is more flexible to provide additional security to different layers [25].The service deployed on the current PaaS may not work properly when the PaaS is updated for the new versions. It may require suitable changes in SaaS which is very critical to the clients and failing which may lead to application failures.

3.1 Security Issues in SaaS

In SaaS, the customer or client is dependent on the service provider for accurate security measures. The service provider must be focussed on the task of protecting multiple users to browse each other's data. So it becomes complicated for the users to make sure that accurate security measures are being followed and it is also critical to believe that the application would be available when needed [21].

The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

- Backup
- Data Breaches
- Data Integrity
- Data Security
- Availability
- Authentication and authorization
- Network Security
- Web application security

a) Backup

The SaaS vendor desires to make sure that all amenable enterprise data is retreated consistently for elegant improvement of quick recovery in case of desolation. The SaaS application also uses strong encryption method to prevent the backup data from inadvertent percolation of accessible information. The users need to separately encode their data and backups so that it may not be retrieved by any unapproved users [23-25].

b) Data breaches

It is fact that the data from different users and organizations resides together in a cloud environment. The chance of breaching into the cloud surroundings will potentially attack the data of all the users. Thus, the cloud becomes a high value intention [23].

c) *Data integrity*

Data integrity is one of the most solemn components in any system. Data integrity is easily attained in a discrete system with a single database. Data integrity in such a system is managed via database transactions [55]. Most of the databases support atomicity, consistency, isolation and durability (ACID) transactions and can preserve data integrity. There are varieties of databases and applications in a distributed system environment. In order to sustain data integrity in a distributed system, transactions across multiple data sources need to be handled suitably in an innocuous manner. One method for confirming the integrity of a set of data is based on hash values. A hash value is retrieved by abbreviating a set of data into a single unique value by way of a pre-demarcated algorithm [26].

d) Web applications security

SaaS application development may imply various types of software components and frameworks. These tools can lessen time-to-market and the cost of renovating a traditional software product or building and deploying a new SaaS solution. One of the obligatory necessities for SaaS applications is that it has to be used and accomplished over the web [27].

e) *Data security*

Data security is one of the chief and most cited issues in SaaS delivery model. As we have already stated that in a conventional on-premise application deployment model, the responsive data of every enterprise reside within the periphery of the enterprise. However, in SaaS model, the venture data is stored outside the enterprise domain i.e., at the SaaS vendor end. That's why; the SaaS vendor requires extra security checks to guarantee data security. Moreover, extra security checks are needed to prevent the breaches occurring due to security susceptibilities in the application or through malevolent employees [15]. This technology requires proper security principles and mechanisms to eradicate the malevolent users. Indeed, in SaaS model most cloud users are constantly anxious regarding their confidential data because it might be used for other malign purposes or transferred to other cloud service providers [46]. The issue of data storage protection in mobile cloud computing is discussed in [17].

f) *Availability*

It should be the major goal of the SaaS application providers to ensure that the systems are in running status and ventures are available with services almost all the time [15]. The availability ensures the steady and timely access to cloud data or cloud computing resources by the appropriate personnel.

This availability issue requires changes in the architecture at the application and infrastructural levels so that high availability and scalability gain can occur. Moreover, flexibility in hardware or software breakdown, as well as the insolence of service strafe should be built in a bottom up manner within the application [28].

g) *Authentication and authorization*

For working with a safe cloud environment the authentication and authorization applications for venture environments may perhaps need to be altered. Forensic tasks may face difficulties since the investigators might not be able to access system hardware physically. A two factor password authentication scheme is introduced by Lio which is based on comprising both the properties of discrete logarithm problem and secure one-way hash function [29].

A mutual authentication scheme based on smart card and password was familiarized by Yang in which firstly, the smart card user registers at the server tailed by choosing a correct client to login, sending access request messages to the server, and lastly the completion of the mutual authentication with the user and thereafter reception of messages can take place .

h) *Network security*

In fact SaaS application treats the vulnerable data attained from the enterprises and stores these data at the SaaS merchant end. The network security encompasses the use of strong network traffic encryption techniques such as the Transport Layer Security (TLS) technique and Secure Socket Layer (SSL) technique [21].

The network layer offers substantial fortification against the customary network security issues e.g., IP spoofing which is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an internet protocol (IP) address indicating that the message is coming from a trusted host. The network layer also offers substantial fortification against port scanning, and packet sniffing. It is worthwhile to mention that the packet sniffer or network sniffer monitors the data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. For peak fortification, Amazon S3 is accessible via SSL encrypted end-points. The encoded end-points are accessible from both the Internet as well as from the Amazon EC2 and it assure that the data is transmitted steadily within AWS and from sources outside of AWS [22].

IV. Cloud Security Solutions

Some famous algorithms are also used in the cloud security are DES, AES, RSA, EC, Blowfish, MD5, SHA-1, SHA-256. These algorithms are well known and been used in the information security for many years. They will solve the same purpose in the cloud what they have been solving in the traditional applications. Using them some techniques have been evolved which useful to secure cloud. These techniques are given as under.

a) Hash Message Authentication Code (HMAC)
b) Third Party Auditor (TPA)
c) Secure Index Management Schemes (SIMS)
d) Provable Data Possession(PDP)
e) Decentralized Information Flow Control (DIFC)
f) Proof of Retrievability (POR)

a) HMAC

The security of HMAC relies on the core hash function used and it is observed that it becomes stronger with SHA-512 but weaker with MD5. A binary authentication code whose length is equal to the length of hash function is the output of HMAC. Furthermore, HMAC intimidate the attacks like forgery and key recovery. However, for the purpose of analysis they characteristically entail a large number of message pairs [25]. In Hash Message Authentication Code (HMAC) process, a secret key and hash algorithm such as secure hash algorithm (SHA) is used to generate the message authentication code. This authentication code firmly provides data integrity and authenticity because the secret key is requisite to replicate the code [25]. HMAC can be helpful against man-in-the-middle attacks on the message. However it is not intended to encrypt the message itself. Moreover, any hash algorithm such as MD5, SHA-1, SHA-256 etc., can be used with HMAC.

b) *TPA*

The technique called Third Party Auditor (TPA) relieves the data owner from the storage and continuance of local data. It also annihilates physical control of data owner from the point of view of storage dependability and security. Moreover, in HMAC an auditing service saves data owner's computation and renders a transparent yet cost-effective method for data owners to achieve trust in the cloud. It eliminates the involvement of the client while the data is being stored in the cloud [29].

c) SIMS

This technique of secure index management was introduced in which the proxy re-encryption technique is used [66]. The secure index management is a cost efficient method. The security of this method depends on pairing which makes it difficult for a vicious third party to decode communication contents [29]. This techniques however faces challenge when distribution of keys are concerned. The Proxy encryption also affects the latency delays due to two phase encryption and decryptions

d) PDP

In this method, the public adaptability is attained by using provable data possession (PDP) and it ensures possession of data files on non-trusted storages [68]. The PDP technique utilizes the RSA-based authenticators for auditing the outsourced data and it recommends the random sampling of few blocks of the file. However, in this method the public audit-ability hassles the linear combination of sampled blocks exposed to the external auditor [30].

e) DIFSC

The decentralized information flow control divide the information flow into a different subdomains and sub entities. The control is not in hands of central authority. This is good way of controlling the damages in the transactional operations. A central authority failure may break the whole operation while decentralized one will give redundancy to the operations and save the systems in case of security attacks.

f) POR

The proof of retrievable (POR) method uses a keyed hash function. In this method, before documenting the data file in cloud storage, the verifier calculates the cryptographic hash by means of keyed hash function. Further, this hash is stored along with the secret key. Thereafter, to verify the accuracy of the file, the verifier consigns the secret key to the cloud chronicles and requests it to calculate and return the value of keyed hash function. The verifier may substantiate the integrity of file for multiple times by storing multiple hash values for various keys [31].

V. CONCLUSION

This paper does an insight into the present status od security in cloud computing. It is evident that one doesn't have to invent a new security algorithms for the cloud but can combine one or many existing secure algorithms to provide security in deployment as well as service models.. The security is however more critical at the Delivery models of the cloud where all Iaas, PaaS and SaaS are to be considered. Not all but some popular security solutions are discussed in the paper

REFERENCES

[1] F. Soleimanian, S. Hashemi, Security challenges in cloud computing with more emphasis on trust and privacy, International journal of scientific and technology research, vol. 1, issue 6, pp. 49-54, 2012.
[2] Gibbs. Steve, Cloud computing, International jurnal of innovative research in engineering and science, vol.1, issue 1,, pp.10-17, 2013.
[3] Mell, Peter, and Tim Grance, The NIST definition of cloud computing, NIST Special Publication, vol.800, page.145, 2011.
[4] Brian, Olivier, Thomas Brunschwiler, Heinz Dill, Hanspeter Christ, Babak Falsafi, Markus Fischer, Stella Gatziu Grivas et al., Cloud computing. White Paper SATW, publish Swiss press Page 6, 2012.
[5] H.Takabi, J.B.D. Joshi, G. Ahn ., Security and privacy challenges in cloud computing environments, IEEE security privacy magazine, vol 8, pp.24-31, 2010.
[6] Garfinkel, Simson L., Technical report : An evaluation of amazon's grid computing services: Ec2, s3 and sqs, Computer science group, Harvard University, Cambridge, Massachusetts, Tech. Rep, 2007.
[7] Rochwerger, B., Breitgand, D. Levy, E. Galis, A. Nagin, K. Llorente,I. M. Montero, R. Wolfsthal, Y. Elmroth, E. Caceres, J. Ben-Yehuda, M. Emmerich, W. Galan, The reservoir model and architecture for open federated cloud computing, IBM Journal of Research and Development vol. 53 page.4, 2009.
[8] Pring. Ben, Cloud computing: the next generation of outsourcing, Gartner Group, pp.1-10, 2010.
[9] Hon. W. Kuan, Christopher Millard, Ian Walden, Negotiating cloud contracts: Looking at clouds from both sides now, Stanford technology law review, vol.16, page.1, 2012.
[10] Fernandes D. A., Soares, L. F., Gomes J. V., Freire M. M., Inácio, P. R., Security issues in cloud environments: a survey, International Journal of information security, vol.13.2, pp.113-170, 2014.
[11] M. Monsef, N. Gidado, Trust and privacy concern in the cloud, European Cup, IT security for the next generation, pp.1-15, 2011.
[12] Zhang, Qi, Lu Cheng, Raouf Boutaba, Cloud computing: state-of-the-art and research challenges, Journal of internet services and applications, vol.1.1, pp.7-18, 2010.
[13] Fernandes, Diogo D. A., Soares, L. F., Gomes J. V., Freire, M. M., Inácio, P. R., Security issues in cloud environments: a survey, International journal of information security, vol.13.2, pp.113-170., 2014.
[14] Velte Toby, Anthony Velte, Robert Elsenpeter, Cloud computing: a practical approach, McGraw-Hill, Inc., 2009.
[15] Nuno Santos, Krishna P. Gummadi, Rodrigo Rodrigues, Towards trusted cloud computing, Proceedings of the 2009 conference on hot topics in cloud computing, pp.3-3., 2009.
[16] Sangroya Amit, Saurabh Kumar, Jaideep Dhok, Vasudeva Varma, Towards analysing data security risks in cloud computing environments, ICISTM, CCIS, 54, Springer Berlin Heidelberg, pp. 255-265., 2010.
[17] Neela, K. L., V. Kavitha, A survey on security issues and vulnerabilities on cloud computing, Int. j. computer. sci. eng. Technol, vol.4 (7), pp.855-860, 2013.
[18] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future generation computer systems, Elsevier B.V, vol.28, pp. 583-592, 2010.
[19] Sriram, Ilango, Ali Khajeh-Hosseini, Research agenda in cloud technologies, arXiv preprint arXiv: 1001.3259, 2010.
[20] Hemant, Palivela, Nitin P., Chawande, Avinash Sonule, Hemant Wani, Development of servers in cloud computing to solve issues related to security and backup, Cloud computing and intelligence systems (CCIS), IEEE international conference, pp.158-163, 2011.
[21] Prasanth A., Bajpei M., Shrivastava V., Mishra R. G., Cloud computing: A survey of associated services, eBook published by HCTL, 2015.
[22] Chou, David C., Amy Y. Chou, Software as a service (SaaS) as an outsourcing model: An economic analysis. Proc. SWDSI'08, pp.386-391, 2007.
[23] Braubach L., Pokahr A., Jander K., Jadex cloud-an infrastructure for enterprise cloud applications, Multi agent system technologies, Springer Berlin Heidelberg, pp.3-15., 2011.
[24] Hashemi, Sajjad, Khalil Monfaredi, Mohammad Masdari, Using cloud computing for e-government: challenges and benefits, World academy of science, engineering and technology, International journal of computer, information science and engineering, vol. 7, no.9 pp. 447-454, 2013.
[25] Domzal J., Securing the cloud: Cloud computer security techniques and tactics (winkler) [book reviews]. Communications Magazine, IEEE, vol.49 (9) pp. 20-20, 2011.

[26] Boniface M., Nasser B., Papay J., Phillips S. C., Servin A., Yang X., Kyriazis D., Platform-as-a-service architecture for real-time quality of service management in clouds., Internet and web applications and services (ICIW), 5th International conference on IEEE, pp.155-160, 2010.
[27] Hashizume K., Rosado D. G., Fernández-Medina E., Fernandez E. B., An analysis of security issues for cloud computing, Journal of internet services and applications, 4(1), pp.1-13, 2013.
[28] Sen, Jaydip, Security and privacy issues in cloud computing, architectures and protocols for secure information technology infrastructures, pp.1-45, 2013.
[29] Sun-Ho Lee, Im-Yeong Lee, Secure index management scheme on cloud storage environment, International journal of security and its applications, vol.9 (2), pp.75-82, 2012.
[30] Ateniese G., Burns R., Curtmola R., Herring J., Kissner L., Peterson, Z., Song D., Provable data possession at un-trusted stores, Proceedings of the 14th ACM conference on computer and communications security, pp.598-609, 2007.
[31] Shacham Hovav, Brent Waters, Compact proofs of retrievability, advances in cryptology-ASIACRYPT, Springer Berlin, Heidelberg, pp.90-107, 2008.