

Security of text data outsourcing in cloud computing

Shristi Bhute^{1*} and Siddhartha Kumar Arjaria²

M.Tech Scholar, Department of Information Technology, TIT, Bhopal¹

Assistant Professor, Department of Information Technology, TIT, Bhopal²

©2016 ACCENTS

Abstract

Cloud computing is a computing based on internet. Demand of cloud computing is increasing day by day. Cloud computing is on demand service with lower cost. Many researches are going on cloud computing. Security breaches are one of the active areas among them. Higher demand and growth leads to security breaches in data outsourcing in cloud computing environment. The main aim of this paper is to review the latest development of a framework which can provide security on text data outsourcing in cloud computing. This paper deals with exploring and analysis different security breaches in cloud Computing. This paper presents and discusses data security along with the access control and authorization. This paper also suggests future enhancement based on the study and analysis.

Keywords

Cloud computing, Security, Data control, Data outsourcing.

1.Introduction

There are several causes why a business enterprises might want to adopt cloud computing. Cloud computing provide ease in applicability and provide on demand service. The two main components of cloud computing are infrastructure and software applications. The first supports the hardware resources like server, storage and network components. The second supports the software applications and computing power for running business applications, as provided by the third parties.

Distributed computing give on intrigue resources in light of pool of benefits available by the cloud suppliers [1] [2] [3]. From the piece of standard enlisting the advantages of dispersed registering are: agility, lower segment cost, device independency, zone independency, and versatility [4] [5]. In any case, the security concerns are the genuine key perspectives later on circulated processing time. There are a couple security majors are displayed in [6], [7], [8], [9], [10], [5]. Virtualization, predominant enrolling are also the more conspicuous office parts of conveyed processing. Regardless, to fulfil the execution on the parallel system and keeping up the respectability is compelling [11].

In each one of these works, staggering tries are made to arrangement courses of action that meet diverse essentials: high arrangement viability, stateless check, unbounded usage of inquiries and misery of data, etc. Considering the part of the verifier in the model, each one of the plans displayed before fall into two classes: private auditability and open auditability [5]. Notwithstanding the way that arranges with private auditability can perform the plans adequately, yet it is trying situation if the data is securing subtly [5]. Virtualization is the key segments of disseminated figuring by which data sharing is possible between different machines of virtual nearness from the server cultivate [12]. Virtualization engages the live migration [9] of virtual machines (i.e. moving a VM beginning with one host then onto the following without cutting it down) which helps in keeping up the ensured SLA to the cloud customer besides to adjust stack across over physical servers in the data centers[12].

The primary cloud suppliers are [13] Google, Microsoft, Amazon and Salesforce.com. The distributed computing benefit display depends on the information correspondence layer. The entire correspondence is depends on three layers. The primary layer is Software as a Service (SaaS) which is for the most part changed on desktop based applications into online programming items that can be utilized around the world. A for the most part used application is Salesforce.com, a customer relationship

*Author for correspondence

organization (CRM) programming for interfacing with associations and clients [14]. As showed by [14] Platform as a Service (PaaS) is a circumstance for Cloud Computing Security Management for making and building applications for different circumstances. As showed by Infrastructure as a Service (IaaS) generally incorporates virtualization circumstances as obtained organizations instead of physical or submitted PC equipment.

In the customary technique for figuring the benefits are gained locally which are occasionally higher in cost and not sensible. This constrains the courses in which a customer could participate with the item in that the item was simply open and accessible for the principal workstation [14]. In any case, now by the usage of conveyed figuring the Software as a Service display has transformed this rationality in a way that item can be purchased for use over the Internet [14]. As opposed to getting programming in a boxed arrangement, the customer can purchase an organization to use an application that is encouraged in the cloud [14]. The standard favorable position of this kind of structure arrives is no need of serious work station as the customer range yet on intrigue resources/programming can give it to rent. So if it is joined with the security organizations it ends up being extreme.

2.Literature survey

In 2011, Ling Zheng et al. [15] differentiating private cloud and open cloud , records differentiates amidst them and advances a building plan of private appropriated registering to support sharp prop, clarifies structure of each layer, and shows thought of private dispersed figuring working structure and framework virtualization. It gives the speculative reference to amass the private appropriated registering, along these lines propels the improvement of the sharp system.

In 2011, Ming Li et al. [16] showed a logical examination using online Personal Health Record (PHR), they first exhibit the need of interest capacity endorsement that reduces the security presentation coming to fruition due to the rundown things, and set up an adaptable structure for Authorized Private Keyword Search (APKS) over mixed cloud data. They then propose two novel responses for APKS in light of a late cryptographic primitive, Hierarchical Predicate Encryption (HPE). Their answers engage capable multi-dimensional catchphrase looks for with achieve request; grant assignment and repudiation of interest capacities. They redesign the request

assurance which covers customers' question catchphrases against the server.

In 2011, Yanjiang Yang et al. [17] recommend that Storage-as-an organization is a critical part of the dispersed figuring system. Database outsourcing is an average utilize circumstance of the dispersed stockpiling organizations, wherein data encryption is an OK approach enabling the data proprietor to hold its control over the outsourced data. Searchable encryption is a cryptographic primitive thinking about private watchword based interest over the mixed database. The setting of huge business outsourcing database to the cloud requires multi-customer searchable encryption, while in every way that really matters each and every current arrangement consider the single-customer setting. To associate this hole, they propose a practical multi-customer searchable encryption arrange for, which has different purposes of enthusiasm over the known approaches.

In 2011, Wang et al. [18] recommended that conveyed figuring has been envisioned as the bleeding edge fabricating plan of IT Enterprise. It moves the application programming and databases to the thought broad server cultivates, where the organization of the data and organizations may not be totally reliable. A maker focuses on the issue of ensuring the respectability of data stockpiling in Cloud Computing. In particular, they consider the task of allowing a pariah controller (TPA), for the advantage of the cloud client, to check the dependability of the dynamic data set away in the cloud. The presentation of TPA slaughters the relationship of the client through the assessing of whether his data set away in the cloud is without a doubt set up, which can be fundamental in finishing economies of scale for Cloud Computing.

In 2012, Syed Naqvi et al. [19] exhibit a formal technique for testing the impact of versatility and heterogeneity on the assembled Cloud security organizations. Their hopes to develop a mean of measuring the impact on security limits under various working conditions and parameters of brought together Cloud courses of action. Their eventual outcomes of this work will help associations with recognizing the best security basic arranging that will fit their Cloud designs and execution requirements.

In 2012, Huaglory Tianfield et al. [20] introduce a thorough study on the troubles and issues of security in dispersed figuring. They first explore the impacts

of the unmistakable traits of disseminated figuring, to be particular, multi-residency, adaptability and pariah control, upon the security requirements. By then, they analyze the cloud security necessities in regards to the primary issues, i.e., protection, respectability, availability, trust, and survey and consistence. They discuss the exploratory order for security issues in disseminated figuring. They plot the security issues in disseminated registering by cloud security assembling plan.

In 2012, Abdullah Abuhussein et al. [21] suggest Healthcare, preparing, business, and various diverse territories look at circulated processing as an attempt to understand the constant inadequacy in volume, establishment, accessibility, and watching quality. Then again, moving data to the cloud proposes moving control of the customer's data to the cloud organization supplier uncertainly. In this manner, the security and insurance of the customer's information transforms into a fundamental issue. Reviewing and taking a gander at among potential circulated registering organizations, speaks to an issue for learner customers interested to move their work to the cloud to pick security decisions that are sufficient and generous meanwhile. They attempts to perceive and arrange an once-over of qualities which reflect the distinctive parts of cloud security and assurance. These attributes can be used to overview and break down circulated registering organizations with the objective that clients can settle on finished choices. Cloud organization suppliers can use them to manufacture and/or offer better cloud courses of action.

In 2012, Wentao Liu et al. [22] recommend that the security issue of appropriated registering is essential and it can keep the quick change of circulated figuring. It exhibits some appropriated processing structures and separates conveyed figuring security issue and its strategy as demonstrated by the disseminated registering thoughts and characters. The data insurance and organization openness in circulated processing are the key security issue. Single security procedure can't handle the appropriated figuring security issue and various customary and new advances and techniques should be used together to ensure the total disseminated processing structure.

In 2013, Nikhilesh Pant et al. [23] exhibit the methodology for cloud allotment and cloud security examination to explore potential security and consistence proposals in cloud environment. They

discusses in inconspicuous component on how an affiliation may proceed for security and consistence examination in the midst of the cloud estimation. Their strategy and thoughts point by point in this paper would be important for affiliations that are incorporated into the cloud gathering prepare.

In 2013, Du meng et al. [24] discusses dispersed registering data security issues, including tile security of data transmission, stockpiling, security and organization of security. Focus on comprehensive data organization impact cloud security examination, and called attention to that a jump forward in the headway of this dispersed processing, endeavor to list the looking at philosophies and whole deal change heading.

In 2013, Fan Yang et al. [25] prescribed that the data security and assurance on cloud is a basic issue, transforming into the best obstruction of conveyed processing headway. A Trusted Cloud Computing Platform (TCCP) in perspective of remote approval builds a trusted cloud for tenant. The essential fragment is fused Trusted Coordinator, taking the spot of tenants to confirm center points independently in appropriated figuring organize. Regardless, when a lot of tenants apply for center points meanwhile, Trusted Coordinator (TC) can't deal with these sales quickly. To address this issue, they propose the establishment of security-level for unmistakable applications in TCCPs, which segments Trusted Coordinator into three, each accountable for affirming different application kind. The particular acceptance plans, for instance, customer mystery word examination, picture hash check and trusted chain estimation, as demonstrated by different security levels. In 2014, Zhao et al. [26] proposed homomorphism encryption calculation in the distributed computing to take care of the issue of information security. As per the creators this can fit for handling and recovery of the encoded information and it is viably pertinent for information transmission and the storage. In 2015, Gupta et al. [27] has been imagined as a front line basic arranging of IT Industries. Security and insurance is the noteworthy snag in the cloud environment as a consequence of its straightforward development displaying. They researches the cloud security risks moreover discuss the ebb and flow security approaches to manage secure the cloud environment.

They also proposed a novel Tri-framework for cloud security against data break which give all around security to the cloud basic arranging.

In 2015, Liu et al. [28] suggest that the existing privacy-preserving rule mining methods only assume a distributed model where every data owner holds the self-data without encryption and together follow a secure protocol to perform rule mining. To address this limitation, they have proposed a novel Protocol for Outsourced Rule Mining (PORM) in this paper. PORM performs rule mining in a cloud environment where data are both encrypted and outsourced.

3. Analysis

The analysis based on the study is shown below. *Figure 1* shows the cloud servers used in the current scenarios. The category wise division is shown in *Figure 1*. *Figure 2* and *Figure 3* shows the public IT services cloud computing distribution, which shows that the application and app are the major portion it means security is the major concern for the data outsourcing.

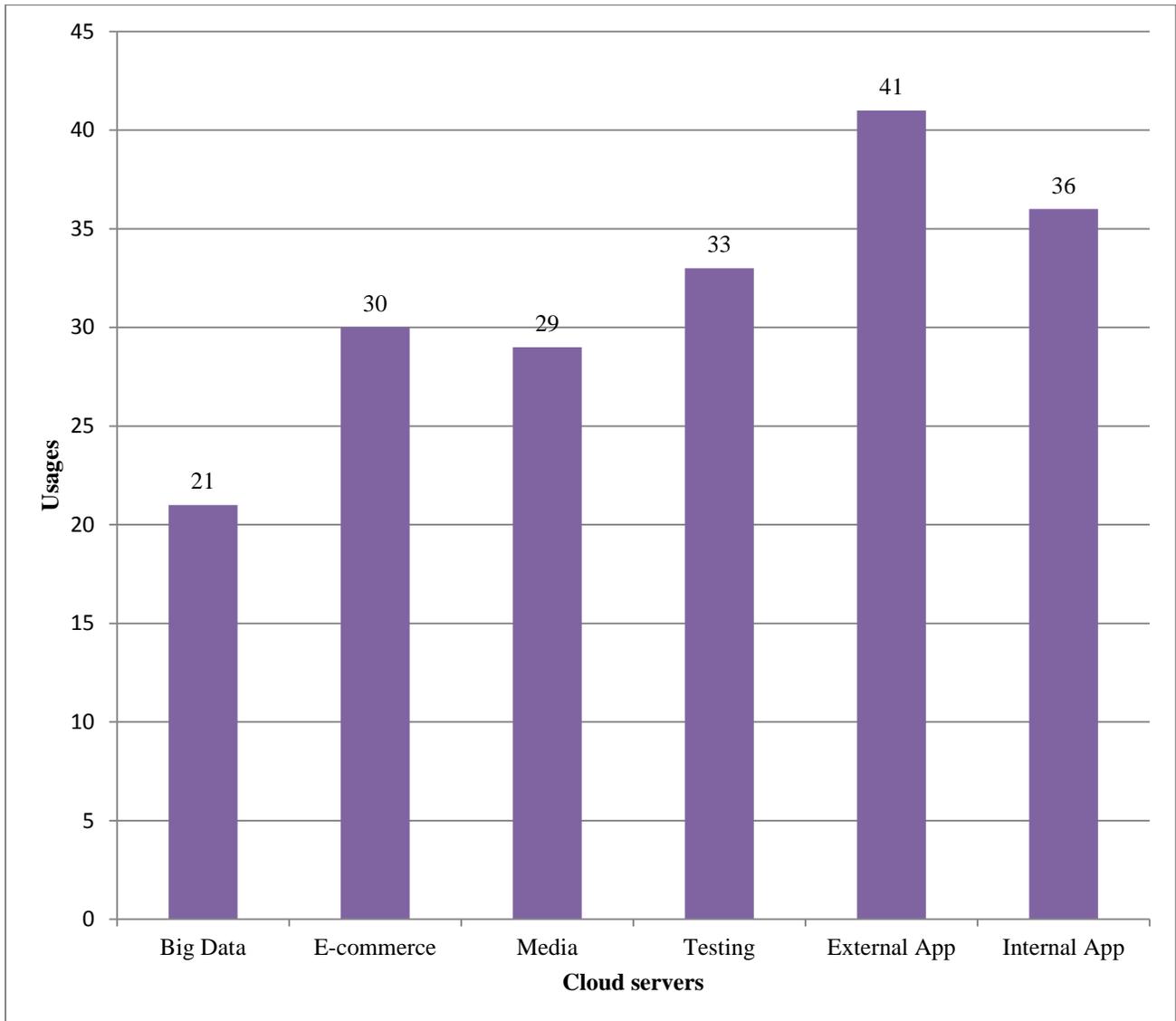


Figure 1 Cloud Servers Use in the current Scenario [29]

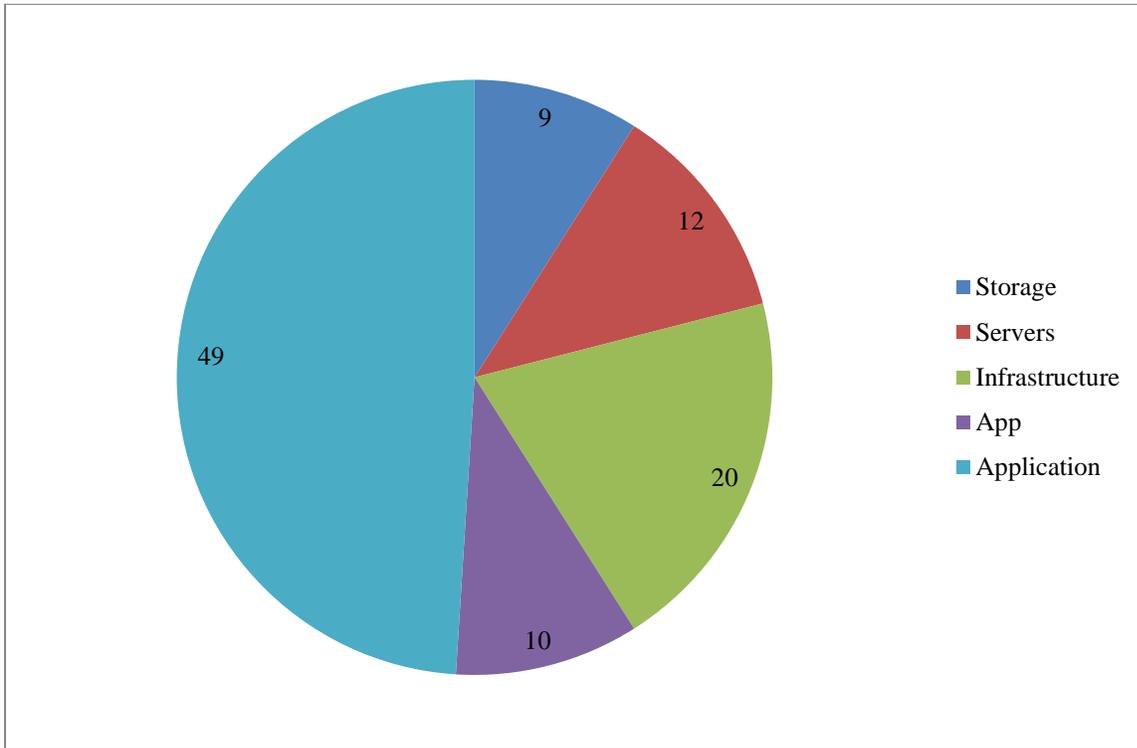


Figure 2 Public IT cloud services distribution, 2009 [30]

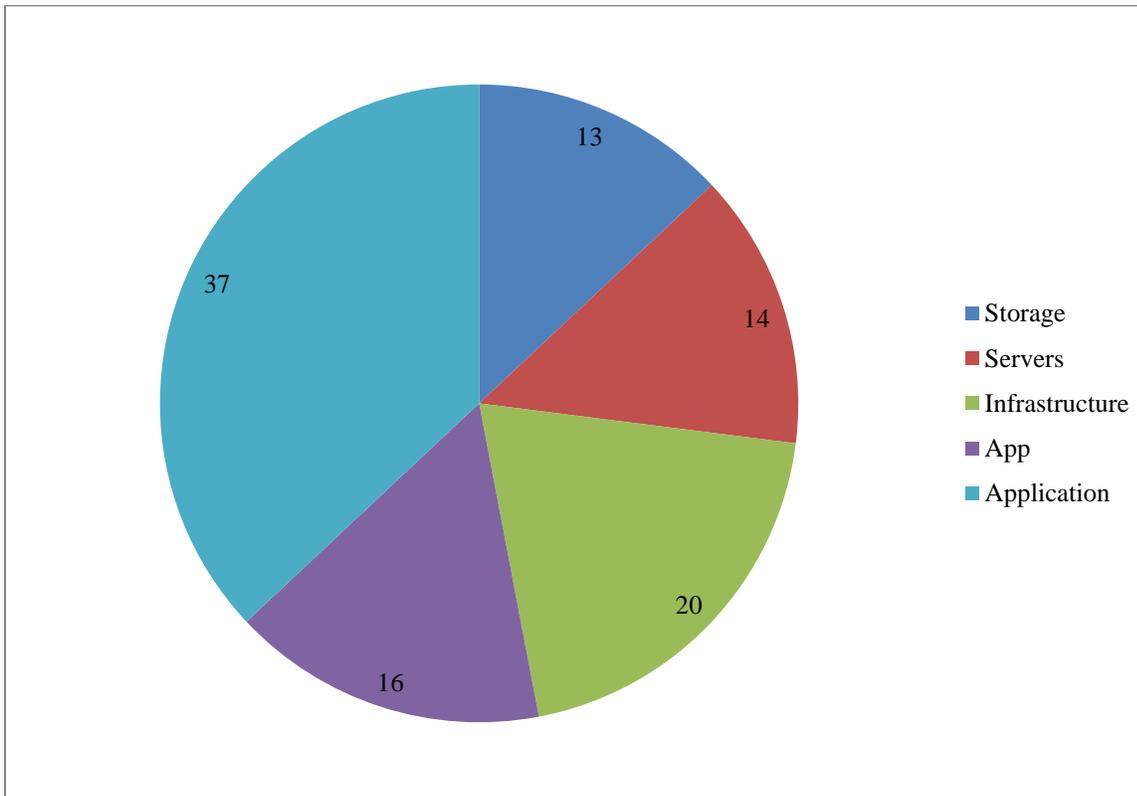


Figure 3 Public IT cloud services distribution, 2014 [30]

4. Problem domain

The following research analysis has been found after the study and observation:

1. There is a need of security when the data is outsourced and it can be notify to the concern.
2. There should be some strong mechanism so that security should be maintained in terms of inter cloud communication.
3. Key should be large and variable number of key is needed for preserving with any kind of malicious behaviour.
4. The data corrupt mechanism can be adopted if any unauthorized access is done.
5. Data protection and categorization protocol can be applied for betterment and enhancement of security.
6. What happen if the data is in unprotected hand? So there should be some safe protocol which can determine all the security steps with the relevant backup and recovery files.

5. Conclusion and future work

This paper deals in the area of data outsource security in cloud computing environment. This paper suggests that there is the need of data security along with the data control and authorization. Different key constraints are found and discussed with some future plan. In future data control with standard encryption techniques can be applied for better security in the mean time for enhancing it. Larger keys should be used with variability will be achieved for preserving with any kind of malicious behaviour.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

- [1] Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. Above the clouds: a Berkeley view of cloud computing. Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS. 2009; 28(13): 2009.
- [2] Ruiz-Agundez I, Peña YK, Bringas PG. Cloud computing services accounting. International Journal of Advanced Computer Research. 2012; 2(4): 7-17.
- [3] Singh A, Shrivastava M. Overview of security issues in cloud computing. International Journal of Advanced Computer Research. 2012; 2(3):41-5.
- [4] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, Song D. Provable data possession at untrusted stores. In proceedings of the 14th ACM conference on computer and communications security 2007 (pp. 598-609). ACM.
- [5] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering (CONSEG) 2012 (pp. 1-8). IEEE.
- [6] Juels A, Kaliski Jr BS. PORs: Proofs of retrievability for large files. In proceedings of the 14th ACM conference on computer and communications security 2007 (pp. 584-97). ACM.
- [7] Shacham H, Waters B. Compact proofs of retrievability. Journal of cryptology. 2013; 26(3): 442-83.
- [8] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. In proceedings of the ACM workshop on cloud computing security 2009 (pp. 43-54). ACM.
- [9] Naor M, Rothblum GN. The complexity of online memory checking. In foundations of computer science, 46th annual IEEE symposium 2005 (pp. 573-82). IEEE.
- [10] Tsai WT, Sun X, Balasooriya J. Service-oriented cloud computing architecture. In seventh international conference on information technology: new generations (ITNG), 2010 (pp. 684-9). IEEE.
- [11] Patra GK, Chakraborty N. Securing cloud infrastructure for high performance scientific computations using cryptographic techniques. International Journal of Advanced Computer Research. 2014; 4(14):66-72.
- [12] Pachorkar N, Ingle R. Multi-dimensional affinity aware VM placement algorithm in cloud computing. International Journal of Advanced Computer Research. 2013; 3(13):121-5.
- [13] http://www.dialogic.com/~media/products/docs/white_papers/12023-cloud-computing-wp.pdf. Accessed 8 April 2016.
- [14] Kembhavi S, Singh G. Auto upload and chi-square test on application software as a service for cloud computing environment. International Journal of Advanced Technology and Engineering Exploration. 2014; 1(1): 26-31.
- [15] Zheng L, Hu Y, Yang C. Design and research on private cloud computing architecture to support smart grid. In international conference on intelligent human-machine systems and cybernetics (IHMSC) 2011 (pp. 159-61). IEEE.
- [16] Li M, Yu S, Cao N, Lou W. Authorized private keyword search over encrypted data in cloud computing. In International conference on distributed computing systems (ICDCS) 2011 (pp. 383-92). IEEE.
- [17] Yang Y. Towards multi-user private keyword search for cloud computing. In IEEE International conference on cloud computing (CLOUD) 2011 (pp. 758-9). IEEE.
- [18] Wang Q, Wang C, Ren K, Lou W, Li J. Enabling public auditability and data dynamics for storage

- security in cloud computing. *IEEE transactions on parallel and distributed systems*. 2011; 22(5):847-59.
- [19] Naqvi S, Michot A, Van de Borne M. Analysing impact of scalability and heterogeneity on the performance of federated cloud security. In *IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom) 2012* (pp. 1137-42). IEEE.
- [20] Tianfield H. Security issues in cloud computing. In *IEEE international conference on systems, man, and cybernetics (SMC) 2012* (pp. 1082-9). IEEE.
- [21] Abuhussein A, Bedi H, Shiva S. Evaluating security and privacy in cloud computing services: a stakeholder's perspective. In *international conference for internet technology and secured transactions 2012* (pp. 388-95). IEEE.
- [22] Liu W. Research on cloud computing security problem and strategy. In *international conference on consumer electronics, communications and networks (CECNet) 2012* (pp. 1216-9). IEEE.
- [23] Pant N, Parappa S. Seeding the cloud in a secured way: Cloud adoption and security compliance assessment methodologies. In *software engineering and service science (ICSESS), 2013 4th International conference on 2013* (pp. 305-8). IEEE.
- [24] Meng D. Data security in cloud computing. In *8th international conference on computer science & education (ICCSE), Colombo 2013* (pp. 810-3). IEEE.
- [25] Yang F, Pan L, Xiong M, Tang S. Establishment of security levels in trusted cloud computing platforms. In *green computing and communications (GreenCom), IEEE and internet of things (iThings/CPSCoM), IEEE international conference on and IEEE cyber, physical and social computing 2013* (pp. 2119-22). IEEE.
- [26] Zhao F, Li C, Liu CF. A cloud computing security solution based on fully homomorphic encryption. In *international conference on advanced communication technology (ICACT) 2014* (pp. 485-8). IEEE.
- [27] Gupta A, Chourey V. Cloud computing: Security threats & control strategy using tri-mechanism. In *international conference on control, instrumentation, communication and computational technologies (ICCICCT) 2014* (pp. 309-16). IEEE.
- [28] Liu F, Ng WK, Zhang W. Encrypted association rule mining for outsourced data mining. In *international conference on advanced information networking and applications (AINA) 2015* (pp. 550-7). IEEE.
- [29] <http://www.prweb.com/releases/cloudsecurity/survey/prweb10225363.htm>. Accessed 8 April 2016.
- [30] <http://www.vi.net/blog/2010/11/the-benefits-of-cloud-computing-to-the-e-commerce-industry/>. Accessed 8 April 2016.