Journal of
Information Technology & Software Engineering

Tabassam, J Inform Tech Softw Eng 2017, 7:5
DOI: 10.4172/2165-7866.1000216

Review Article Open Access

Security and Privacy Issues in Cloud Computing Environment

Shazia Tabassam*

Department of Computer Science, University of Agriculture, Faisalabad, Pakistan

Abstract

Cloud computing turned into the most predominant innovation in recent years. This innovative technology provides services to the customers for software and hardware. One can state that distributed computing can blast the portable business. Cloud computing is a basic technology for sharing of resources on the internet. Virtualization is a central innovation for empowering cloud resource sharing. Confidentiality of data storage is the essential alarm for assurance of data security so cloud computing does not provide robust data privacy. All details of data migration to cloud remain hidden from the customers. The problem in cloud computing environments are security of cloud computing. In this exploration we tended to the difficulties in fulfilling of cloud computing environment regarding security hazard implementation strategies on cloud computing environment and comparison of different cloud computing architecture through comparative study. In this paper a survey of the different security hazards that represent a danger to the cloud is presented. This paper is a review more particular to the different security issues that has radiated because of then a nature of the administration conveyance models of a cloud computing framework.

Keywords: Confidentiality; Virtualization; Robust; Exploration

Introduction

Business companies are came to know about this factor that cloud computing [1] is providing the most fast access to the infrastructure and services over internet. Gartner defines cloud computing as "a style of computing where massively scalable IT enabled capabilities are delivered 'as a service' to external customers using Internet technologies". Cloud providers currently enjoy a profound opportunity in the marketplace. The providers must ensure that they get the security aspects right, for they are the ones who will shoulder the responsibility if things go wrong. The cloud offers several benefits like fast deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services. While the cloud offers these advantages, until some of the risks are better understood, many of the major players will be tempted to hold back. According to a recent IDCI survey, 74% of IT [2] executives and CIO's cited security as the top challenge preventing their adoption of the cloud services model [3]. Analysts' estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12% of the worldwide software market will move to the cloud in that period. To realize this tremendous potential, business must address the privacy questions raised by this new computing model. Cloud computing created a powerful effect in academia and IT industry. Basically, it intends to harden the money related utility model with the transformative change of many existing approaches and figuring advances, including appropriated organizations, applications, and data structures involving pools of PCs, frameworks, and limit resources. Ambiguities exists in IT people group about how a cloud varies from existing models and how these distinctions affect its reception. Some observe a cloud as a novel specialized insurgency, while others think of it as a characteristic advancement of innovation, economy, and culture. By and by, distributed computing is a critical worldview, with the possibility to fundamentally decrease costs through streamlining and expanded operating and monetary efficiencies. Furthermore, distributed computing could altogether improve cooperation, nimbleness, and scale, therefore engaging a really overall processing model over the Internet system. Regardless, without appropriate security and insurance courses of action expected for clouds, this possibly changing handling perspective could transform into an enormous dissatisfaction. A couple investigations of potential cloud adopters show that security and assurance is the fundamental concern blocking its selection issues in cloud security could be as DDos denial of service attack and Worm containment. In the world of computing, clients are all around required to acknowledge the basic preface of trust. Actually, some have guessed that trust is the greatest concern confronting distributed computing. No place is the component of trust more evident than in security, and many trust and security to be synonymous. Here, I inspect some security issues and the related administrative and lawful worries that have emerged as distributed computing rises as an essential dispersed registering stage. The idea of distributed computing has been advancing for more than 40 years. In the 1960s, JCR Licklider presented the expression "intergalactic PC organize" at the Advanced Research Projects Office. This idea served to present the idea that the world came to know as the Internet [4]. The basic preface was a worldwide interconnection of PC projects and information. The expression "cloud" starts from the broadcast communications universe of the 1990s, when suppliers started utilizing virtual private arrange (VPN) administrations for information correspondence. VPNs kept up a similar data transfer capacity as settled systems with impressively less cost: these systems bolstered dynamic steering, which took into account an adjusted usage over the system and an expansion in transmission capacity proficiency, and drove to the authoring of the expression "telecom cloud". Cloud processing's preface is fundamentally the same as in that it gives a virtual processing condition that is powerfully assigned to address client issues. From a specialized viewpoint, distributed computing incorporates service oriented engineering (SOA) and virtual utilizations of both equipment furthermore, programming. Inside this condition, it gives a versatile administrations conveyance stage. Cloud figuring offers its assets among a billow of administration purchasers, accomplices, and merchants. By sharing assets at different levels, this

***Corresponding author:** Shazia Tabassam, Department of Computer Science, University of Agriculture, Faisalabad, Pakistan, Tel: +923356850545; E-mail: shazi7744@gmail.com

Received November 10, 2017; **Accepted** November 29, 2017; **Published** December 06, 2017

Citation: Tabassam S (2017) Security and Privacy Issues in Cloud Computing Environment. J Inform Tech Softw Eng 7: 216. doi: 10.4172/2165-7866.1000216

stage offers different administrations, for example, a foundation cloud (for instance, equipment or IT framework administration), a product cloud (for example, programming, middleware, or conventional client relationship administration as an administration), an application cloud (application, UML demonstrating devices, or interpersonal organizations as an administration), and a business cloud.

The Cloud Security Alliance has distinguished a couple of basic issues for trusted distributed computing, also, a few late works examine the most basic issues on cloud security and privacy. Public also, private mists request diverse levels of security requirement. We can recognize between various administration level assentions (SLAs), by their variable level of shared obligation among cloud suppliers and the clients. Basic security issues incorporate information honesty, client secrecy, what's more, trust among suppliers, person clients, and client bunches. The three most mainstream cloud benefit models have shifting security requests. The framework as-an administration (IaaS) demonstrate sits at the deepest execution layer, which is stretched out to frame the stage as-aservice (PaaS) layer,by including OS and middleware bolster. PaaS additionally stretches out to the programming as-an administration (SaaS) show by making applications on information, substance, and metadata utilizing extraordinary APIs. This infers SaaS requests all insurance capacities at all levels. At the other outrageous, IaaS requests security for the most part at the systems administration, put stock in registering, furthermore, figure/stockpiling levels, though Paas exemplifies the IaaS bolster in addition to extra assurance at the asset administration level. Distributed computing is a developing innovation which gives the facility of resources sharing for example software and hardware and servers over internet. But there are some issues in the security and privacy of data cloud is not as secure as compare to traditional IT operations, security patching is much better in cloud, Demonstrating compliance is harder in cloud, Loss of data is less in clouds, Security will be enhanced by more control power. Insecure apps can be handled by cloud providers in better way than the users. There is a basic need to safely store, oversee, share and examine enormous measures of complex information, to decide examples and patterns keeping in mind the end goal to enhance the nature of human services better defend, the country and investigate elective vitality. As a result of the unpredictable method for the applications, it is basic that fogs be secure. The guideline security challenge with clouds is that, the information proprietor might not have control of, where the information is put. This is a result of the reality, on the off chance that one needs to abuse, the advantages of utilizing distributed computing, one should likewise use the asset assignment and the booking given by mists. Subsequently we have to defend, the information amidst untrusted forms. The creating disseminated processing model attempts to address the unsteady improvement of web-related devices, and handle tremendous measures of data. Google has now displayed the Map Reduce framework for taking care of a considerable measure of data on item hardware". Apache's Hadoop" cloud computing framework is developing as a predominant programming segment for distributed computing consolidated with coordinated parts, for example, MapReduce. There are several of security problems for cloud computing, as it is surrounded by numerous technologies in addition of 'networks databases', 'working structures', 'virtualization resource booking', 'trade organization', 'stack changing', concurrence control, and memory organization [5]. Henceforth, security issues for different of these structures and developments are material to circulated registering. For example the framework that interconnects the structures in a cloud must to be secure. Virtualization in conveyed figuring realizes a couple security interest. For example, mapping the virtual machines to the physical machines must be done securely. Data security incorporates scrambling the data and moreover ensuring that legitimate systems are executed for data sharing. What's more, resource dissemination and memory organization figuring's must be secure. At long last, information mining strategies might be relevant to malware discovery in mists. Information may misfortune or might be a there will be a danger of record capturing information ruptures risk is additionally a security concern.

Characteristics of Cloud Computing

There are five fundamental attributes of the distributed computing which make the cloud driving more suitable innovation for information stockpiling and utilizing the assets over web [6].

Self-service on demand

A customer can independently arrangement, figuring limits, for instance, server time and framework or system stockpiling, as required therefore without requiring human coordinated effort with every master association.

Pooling of resources

The supplier's processing assets are pooled to serve different customers using, a multi occupant demonstrate with different physical and virtual assets effectively doled out and reassigned by shopper ask. There is a sentiment territory self-rule in that the customer generally has no control or data over the right region of the given assets yet may have the ability to decide region at a more hoisted measure of thought. Instances of benefits consolidate stockpiling, taking care of, memory and framework transmission limit.

Broad network access

Capacities are available over the structure and access to through standard methodology or instrument that actuate use by heterogeneous thin or thick client stages (e.g., cell phones, tablets, adaptable PCs and workstations) (Figure 1).

Rapid elasticity

Capacities can be adaptably provisioned, and discharged some of the time consequently, relative rapidly outward and inside comparable with demand. For the customer, the capacities available for provisioning much of the time radiate an impression of being limitless and can be appropriated in any sum at whatever point.

Measured service

Cloud frameworks automatically control and upgrade, cloud resource use by utilizing a metering ability at the level of abstraction suitable to the kind of administration (e.g., stockpiling, planning, exchange speed and dynamic customer accounts). Resource use can be observed, controlled and revealed, giving straightforwardness to the supplier and customer.

Cloud Computing Models

There are three basic models introduced by cloud computing SAAS, IAAS, and PAAS, SAAS stands for software as a service, IAAS stands for infrastructure as a service and PAAS stands for platform as a service [7].

Software as a service

Software as a service is a facility or service model of cloud which offered an on-request online subscription of software. Likewise with the other cloud service models, "SaaS" offers organizations the chance to decrease inward IT bolster expenses and exchange upkeep obligation

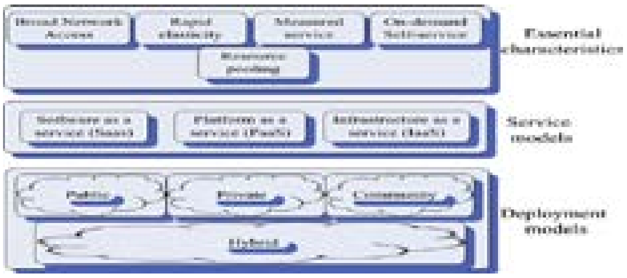

Figure 1: NIST definition of cloud computing.

to the SaaS supplier. SaaS is by a long shot the most generally utilized cloud conveyance show on the grounds that practically every product merchant is hoping to put its offering on the Saas rails there are Saas offerings in each class of programming items, and it would presumably take days to rundown all Saas programming sellers in this paper**.**

Platform as a service

PaaS (Platform as a Service) is a cloud service model which provides clients with a configurable application stage including a pre-introduced programming stack. PaaS can be seen as another reflection layer over the equipment, working framework, and virtualization stack. The PaaS demonstrate conveys noteworthy incentive to organizations since it decreases multifaceted nature of foundation and application upkeep and permits focusing on center programming improvement capabilities. As said in the presentation section, the cost of programming improvement in vast associations is normally lower than the cost of programming and foundation support. Obviously, organizations are progressively inspired by streamlining their application and middleware frameworks with a specific end goal to enhance efficiency and limit related operational costs.

Infrastructure as a service

Foundation as an administration encourages associations to move their physical structure to the cloud with a level of control like what they would have in a traditional on-initiate datacenter. IaaS gives the storage room likeness to the in-house datacenter stood out from various organizations sorts. Center datacenter framework segments are capacity, servers (registering units), the system itself, and administration apparatuses for foundation upkeep and checking. Each of these parts has made a different market specialty. While some little organizations have practical experience in just a single of these IaaS cloud specialties, vast cloud suppliers like Amazon or Right Scale have offerings over all IaaS territories.

Cloud Security Issues

There are many security issues in clouds as they provide hardware and services over the internet [8].

Data breaches

Cloud providers are the attractive target for the hackers to attack as massive data stored on the clouds. How much severe the attack is depend upon the confidentiality of the data which will be exposed. The information exposed may be financial or other will be important the damage will be severe if the exposed information is personal related to health information, trade secrets and intellectual property of a person of an organization. This will produce a severe damage. When data breached happened companies will be fined some lawsuits may also occur against these companies and criminal charges also. Break examinations and client warnings can pile on critical expenses. Aberrant impacts, for example, mark harm and loss of business, can affect associations for a considerable length of time. Cloud suppliers commonly convey security controls to ensure their surroundings, in any case, associations are in charge of ensuring their own information in the cloud. The CSA has suggested associations utilize multifaceted confirmation and encryption to ensure against information ruptures [9].

Network security

Security data will be taken from enterprise in Saas and processes and stored by the Saas provides. To avoid the leakage of the confidential information Data all over the internet must be secured. Strong network traffic encryption will be involved to secure the network for traffic**.**

Data locality

Consumer's uses Saas applications in the Saas environment provided them by the Saas providers and also processing of their data. In this case users or clients of clouds are unaware of the fact that where their data is getting stored. Data locality is much important in May of the countries laws and policies regarding the locality of data are strict**.**

Data access

Data on clouds must be accessible from anywhere anytime and from any system. Cloud storages have some issues regarding the access of the data from any device [10]. Information breaks and different sorts of assaults flourish in situations with poor client verification and frail passwords. Take a gander at the genuine assault on Sony that happened only a few years back. They are as yet feeling the budgetary and social impacts of the hack, which to a great extent succeeded on account of administrators utilizing feeble passwords. The cloud is a particularly appealing target since it exhibits a concentrated information store containing high-esteem information and brought together client get to. Utilize enter administration frameworks in your cloud condition, and be sure that the encryption keys can't without much of a stretch be discovered on the web. Require solid passwords and place teeth in the prerequisite via consequently turning passwords and different methods for client ID. To wrap things up, utilize multi-figure validation.

DoS attacks

One cannot stop the denial of service attacks because it is not possible one can mitigate the effect of these attacks but cannot stop these attacks. DoS assaults overpower resources of a cloud service so clients can't get to information or applications. Politically roused assaults get the front features, however programmers are similarly prone to dispatch DoS assaults for pernicious goal including extortion. What's more, when the DoS assault happens in a distributed computing condition, process burn charges experience the rooftop. The cloud supplier ought to invert the charges, yet consulting over what was an assault and what wasn't will take extra time and irritation. Most cloud suppliers are set up to deny DoS assaults, which takes consistent observing and moment alleviation.

System vulnerabilities

Vulnerabilities of the system are exploitable program bugs in the OS that programmers intentionally use to control or invade a PC framework. Fortunately, essential IT cleanliness goes far towards shielding you from this sort of genuine assault. Since machines exist in your cloud supplier's server farms, be sure that your supplier hones normal weakness examining alongside convenient security fixes and overhauls.

Account hijacking

You may have seen an email that looks true legitimate. You tap on a connection, and soon thereafter sirens blast and cautioning lights streak as your antivirus program goes to fight. Or, then again you may have been genuinely unfortunate and had no clue that you were recently the casualty of a phishing assault. At the point when a client picks a powerless secret key, or taps on a connection in a phishing endeavor, they are at genuine danger of turning into the channel for genuine risk to information. Cloud-based records are no special case. Foundation solid two variable validation and computerize solid passwords and watchword cycling to help secure yourself against this sort of digital assault.

Malicious insiders

Most information loss or harm happening inside an association is human mistake. noxious insiders do exist and they do much of harm. A malicious insider may be a present or previous worker, contractual worker, or accomplice who has the accreditations to get to organization information and intentionally uses, takes, or harms that information. Resistance fixates on secure procedures, for example, solid get to control, and always screen forms and explore activities that lie outside the limits of adequate capacities.

The APT parasite

Additionally called APTs, programmers plan these long term cyber-attacks to give them continuous access into a system. Cases of section focuses incorporate phishing, introducing assault codes by means of USB gadgets, and interruption by means of unreliable system get to focuses. Once in, the interruption shows up as ordinary system movement and the aggressors are allowed to act. Mindful clients and solid get to controls are the lines of best safeguard against this kind of assault.

Permanent data loss

Any information destruction or loss can be a permanent harm to the business. Cloud information is liable to an indistinguishable dangers from is on premise information: unintentional cancellation by clients or staff of providers, natural loss or damage, or psychological militant assault. It is the cloud supplier's obligation to make preparations for human mistake and to fabricate strong physical server farms. In any case, IT should likewise secure against cloud information misfortune by setting up SLAs that incorporate incessant and obvious reinforcement to remote locales, and encoding records in the event of inadvertent information introduction [11].

Shared technology, shared dangers

Cloud suppliers allow administrations to thousands to a huge number of occupants. Administrations run from cloud reinforcement to whole framework, stage, and applications as an administration. The supplier ought to plan their engineering for solid separation in multitenant designs: a fruitful assault on one client is sufficiently terrible. A multitenant assault that spreads from one client to thousands is a debacle. When you take a gander at cloud supplier and multitenant administrations, ensure that they have executed multifaceted validation on all server has and work present day interruption location frameworks.

Compromised credentials and broken authentication

Many cloud applications are equipped towards client collaboration, however free programming trials and join openings open cloud administrations to pernicious clients. A few genuine assault sorts can ride in on a download or sign in: DoS assaults, email spam, computerized click extortion, and pilfered substance are only a couple of them. Your cloud supplier is in charge of solid episode reaction structures to distinguish and remediate this wellspring of assault. IT is in charge of checking the quality of that structure and for observing their own cloud condition for manhandle of resources.

Hacked interfaces and APIs

APIs and UIs are the backbone of cloud computing connections and integration amongst clients and distributed computing. Cloud APIs' IP addresses uncover the association amongst clients and the cloud, so securing APIs from irruption or human mistake is basic to cloud security. Work with your cloud supplier and application merchants to construct information streams that don't open APIs to simple assault. Put resources into applications that model dangers in a live situation, and practice visit entrance testing.

Solution to Security Issues

There are many security issues in the security of cloud computing which are need to be resolved in order to make clouds more secure to check the security of a cloud the following areas must be consulted with the cloud service providers.

Written security policies plan

If the cloud service providers have a written security plan of policies then the security of the data will be guaranteed, if the cloud service provider do not have a security policies written plan then the cloud is not safe and security of the data cannot be guaranteed as they do not have a written plan of security policies. This means that their data security program development. Organizations that have not formalized their security strategies cannot be trusted with your touchy corporate/client information. Strategies shape the system and establishment and without security is just an idea in retrospect

Multifactor authentication

If the cloud providers provide the multifactor authentication for example one time password and mobile [3] code then the security of the data will be more tight as it will be protected by multi factors. If someone try to unlock the data through password one time wrong password will be sent to the data owner at his or her mobile so that he can authenticate the login to the data [12]. Multifactor authentication make the level of protection of data more high.

Access to data

Data of enterprise must be accessed and seen by the administration not by the users. This access will provide the enhance security to the data over the cloud. Many cloud applications are equipped towards client collaboration, however free programming trials and join openings open cloud administrations to pernicious clients. A few genuine assault sorts can ride in on a download or sign in DoS attacks, email spam, computerized click extortion, and pilfered substance are only a couple of them. Your cloud supplier is in charge of solid episode reaction structures to distinguish and remediate this wellspring of assault. IT is in charge of checking the quality of that structure and for observing their own cloud condition for manhandle of resources.

Appropriate cloud model for business

Appropriate cloud model for business will be private cloud. Private cloud are more costly than public clouds but more secure. As they are costly they are more secure. Private clouds are only used by only one organization and security level is higher than the public cloud. As business contains confidential information and financial transactions and business secrets more security is needed hence private clouds are safer than public clouds.

Encryption of backups

Cloud backups of data must be encrypted otherwise encryption of data does not have any meaning if the backups of data are not encrypted. Any of the hacker can get access to these backups if they are not protected with appropriate encryptions. If the backups are not encrypted data is not secure. An untested reinforcement is a futile reinforcement. A decoded reinforcement overcomes the security controls in the generation condition. Data should be secured over its whole lifecycle.

Regulatory compliance

Contingent on business prerequisites an organization's foundation could be liable to certain complicity related. Organizations ought to have a reasonable rundown of consistence prerequisites before considering cloud specialist co-op's consistence directions may fluctuate from area related others secure.

Formal change control process

If the organization have a formal control process change then the cloud is fast and secure for the time sensitive data. If the organization do not have a formal change process control during the regular up gradations then their servers will goes down no one can access the data. And if the data is time sensitive than these cloud which do not have formal change process control they are not safe for tie sensitive data. Organizations that execute changes and setup in a specially appointed way will probably encounter huge downtime in their condition. The main source of system blackouts can be credited to lack of foresight and absence of progress control. In the event that the information you are sending to the cloud is time delicate, you need to run with a supplier that submits to a formal change control handle, hence dealing with the inborn hazard in impromptu changes.

Are external third-party contracts and agreements

Like the idea of subcontracting, in the event that you endow a cloud merchant with your data and they thus utilize another supplier (to store your data for instance) does the underlying seller guarantee that their accomplices follow the arrangements and security understandings that were laid out in your agreement? If not, these accomplices debilitate the general security of the data chain.

Secure data destruction

Secure destruction of data is necessary when needed. If the destruction of data is not secured then the risks of data leakage are present. Anyone can retrieve that data when the data is not destructed safely. In the event that you are putting away classified/delicate information in the cloud and if the seller does not appropriately pulverize information from decommissioned gear, the information is unnecessarily put at hazard. Get some information about their information annihilation handle.

Encryption scheme design and test

If the encryption schemes designed and tested by the professional and experienced persons then the security of the cloud is of trust. A questionnaire was designed and conducted to test the security issues and their solution and the level of security. The respondents of this questionnaire were cloud service providers and cloud users who have expertise and experience in cloud environments.

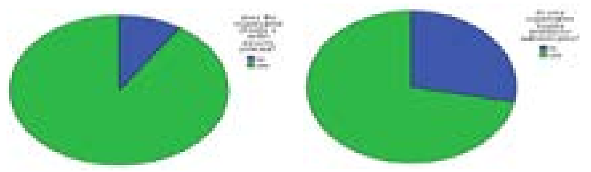

Figure 2: Cloud providers are providing the written security policies document.

In this Figure 2, some of the results shown which describes If the organization or cloud providers are providing the written security policies document then this will assure the security of data. Here the graph shows that most of the companies are providing the written security policies. Rest of the companies with answer “no” are not providing the written security policies which means there is no guarantee of the security of data as they do not even providing the written policies of their security plan. If the cloud providing companies are providing the multifactor authentication then the level of security is up to standard. As one type password and code on cell phone secure the data more tightly. Graphs shows that many of cloud providers are providing multifactor authentication and rest of them are not using the multifactor protection technique. If the cloud providing companies are providing the multifactor authentication then the level of security is up to standard. As one type password and code on cell phone secure the data more tightly. Graphs shows that many of cloud providers are providing multifactor authentication and rest of them are not using the multifactor protection technique. If backups of data are encrypted then the data is secured otherwise no security of the data means at all as there backup are not encrypted. Graph shows that most of the companies provide backup encryptions. If the organization have a formal control process change then the cloud is fast and secure for the time sensitive data. If the organization do not have a formal change process control during the regular up gradations then their servers will goes down no one can access the data. And if the data is time sensitive than these cloud which do not have formal change process control they are not safe for tie sensitive data.

Conclusion

Cloud computing technology is the emerging technology which provide the facilities of software and hardware over internet on demand. A less expensive technology to share the resource over internet. It is a technology that is based on internet. Despite of many advantages there are lots of issues in cloud computing environment regarding the security of the clouds transactions and data storage over internet. As cloud users do not know where there data is going to secure and how much it is secured. Is it safe to move data on clouds what will be the standards of security to get the services from the cloud providers. In this research I tried to find out the security issues in cloud computing environment and which the good architectures for computation are. This research will help the cloud users to understand the security level of cloud computing whether it is safe to migrate to cloud and what standards must be checked before migrating to clouds. Hence clouds are safe to store data.

References

1. Ali M, Khan SU, Vasilakos AV (2015) Security in Cloud Computing: Opportunities and Challenges. Inf Sci 305: 357-383.

2. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2009) Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing

as the 5th Utility. Future Gener Comput Syst 25: 599-616.

3. Dinh HT, Lee C, Niyato D, Wang P (2013) A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches. Wirel Commun Mob Comput 13: 1587-1611.
4. Guba EG, Lincolin Y (1994) Competing Paradigm in Qualitative Research. Handbook of Qualitative Research 4: 105-117.
5. Ferretti L, Colajanni M, Marchetti M (2014) Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases. IEEE Trans Parallel Distrib Syst 25: 437-446.
6. Höfer CN, Karagiannis G (2011) Cloud Computing Services: Taxonomy and Comparison. J Internet Serv Appl 2: 81-94.
7. Gorelik E (2013) Cloud Computing Models. MIT Sloan School of Management.
8. Huang X, Liu JK, Tang S, Xiang Y, Liang K, et al. (2015) Cost-effective Authentic and Anonymous Data Sharing with Forward Security. IEEE Trans Comput 64: 971-983.
9. Garbarino S, Holland J (2009) Quantitative and Qualitative Methods in Impact Evaluation and Measuring Results. GSDRC Emerging Issues Research Service, pp: 1-59.
10. He D, Wang H, Zhang J, Wang L (2017) Insecurity of an identity-Based Public Auditing Protocol for the Outsourced Data in Cloud Storage. Inf Sci 375: 48-53.
11. Hao Z, Zhong S, Yu N (2011) A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability. IEEE Trans Knowl Data Eng 23: 1432-1437.
12. Fernando N, Loke SW, Rahayu W (2013) Mobile Cloud Computing: A Survey. Future Gener Comput Syst 29: 84-106.