Journal of Advances and Scholarly Researches in Allied Education
Vol. 17, Issue No. 2, October-2020, ISSN 2230-7540

A Review of Cloud Services and Characteristics of Cloud Computing and its Security Mechanism

Saket Nigam[1]*, Dr. Rajeev Yadav[2]

[1] Research Scholar, Shri Krishna University, Chhatarpur M.P.

[2] Professor, Shri Krishna University, Chhatarpur M.P.

Abstract - Cloud computing is a fast developing industry, with widespread adoption among both consumers & businesses. Cloud computing's popularity has skyrocketed since its inception, which can be traced back to the early days of grid & utility computing. The convenience of being able to access data from any location at any time is a major selling point of cloud computing. Email clients like Hotmail & Gmail, document editors like Google Docs, program creators like Google App Engine, & cloud storage solutions like Amazon S3, Google Drive, & Windows SkyDrive all see heavy usage. In the early days of the Cloud, Amazon EC2/S3 was one of the initial widely adopted services. Data sharing is made possible via cloud computing, which can increase the user's efficiency and output.

Keywords - Cloud computing, Security, Data Sharing, Cloud Services, Security Mechanism.

----------X----------

INTRODUCTION

"According to NIST, "cloud computing" is "a technology that offers convenient, on-demand configurable computing resources pool of configurable computing resources (e.g., networks, virtual machines, storage, applications, & services) that could be rapidly provisioned, released, & paid for with minimal management effort or service provider interaction."

Cloud computing is a technology offering services in which resources are provisioned on an on-need, pay per use basis through web-based tools and applications, as opposed to a direct connection to a server (Investopedia). Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing allows configuring, manipulating, and accessing the resources over the network. Fig 1 shows the cloud computing architecture.

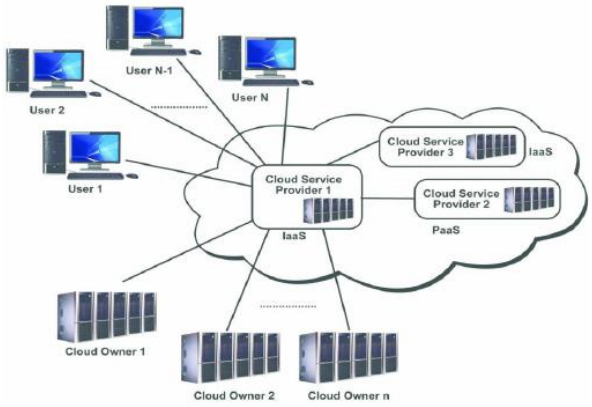

Figure 1: Cloud Computing Architecture

With the advent of cloud any business, organization, university, research centre etc. can reduce their capital expenditure and instead divert the investment to other areas thereby strengthening their organizations. The employees in an organization can share their data through cloud. The research community has benefitted a lot because of sharing their research works through cloud. The major features of the cloud are ubiquity, resource pooling and elasticity, adaptability, scalability, flexibility, multi-tenancy and high Quality of Service (QoS). Main reasons to use cloud computing are, maintaining or managing the network does not need any effort while it provides flexible capacity and Internet access from any place. Advantages of cloud computing include improved performance, instant software updates, quick deployment, easy access

to information, efficient backup and recovery, reduced cost and does not require capital expenses. When it comes to providing cloud services the various corporate players are: Amazon web services, Google Cloud, Microsoft Azure, Salesforce etc.

CLOUD CHARACTERISTICS

In specifically, there is elaboration on five key aspects of cloud computing:

On-demand self-service, as depicted in Fig2 by Tharam Dillon, Chen Wu, & Elizabeth Chang (2010): a consumer with a time-sensitive need can automatically take advantage of computing properties (including CPU time, network storage, software use, and so on) without engaging in human interactions with providers of these resources. proves that resources could be accessed independently of the service provider in a scenario where those resources are pooled.

Figure 2: On-demand Access

Broad network access: As described by Tharam Dillon, (2010) in Fig3 Shows that cloud materials can be shared by application running on different platforms., these computing resources are dispersed over networks (namely the Internet) &utilised by numerous client applications on a variety of platforms (like mobile phones, laptops, & PDAs) situated at a consumer's site.

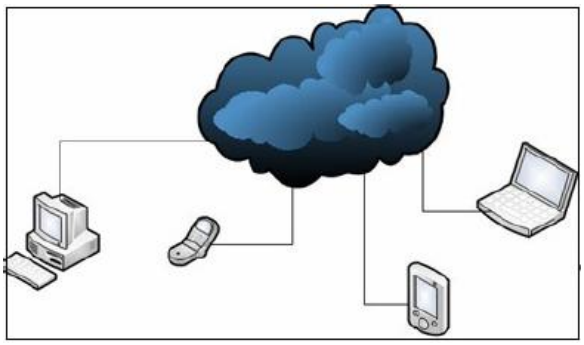

Figure 3: Broad networks Access

Resource pooling: A cloud computing supplier's processor assets are "pooled", formed in an effort to aid clients utilizing either the multitenure or the virtualization model, "with dissimilar physical & virtual assets constantly divided & reallocated presenting to client claim". The motivation for setting up such a pool-based processing standard lies in two important elements: economies of scale & specialization. As a result of using a pool-based strategy, physical resources become "undetectable" to customers since they lack access to information regarding the location, acquisition, or maintenance of these assets (e.g. database, CPU, and so on.). The location of a customer's data in the Cloud is not something they can easily ascertain. It is shown in Fig.4 that virtualization, as explained by Tharam Dillon, (2010) allows the administration provider's figuring assets to be stored in a centralized location & shared across multiple clients.

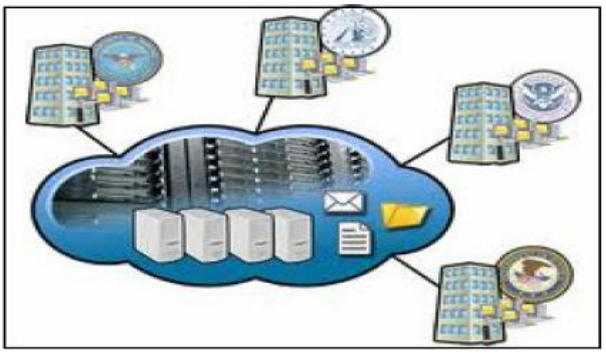

Figure 4: Pooled Resources

Rapid elasticity: Customers no longer need to wait for assurance & agreement before using computer assets to scale up or down; instead, they can do it whenever they like. Moreover, the availability of resources appears infinite to them, despite the fact that the consumption rate may unexpectedly climb to its maximum limit. As mentioned by Tharam Dillon (2010), Fig 5 demonstrates how cloud users can quickly & effectively increase or decrease the amount of available computing resources to fit the needs of their businesses.

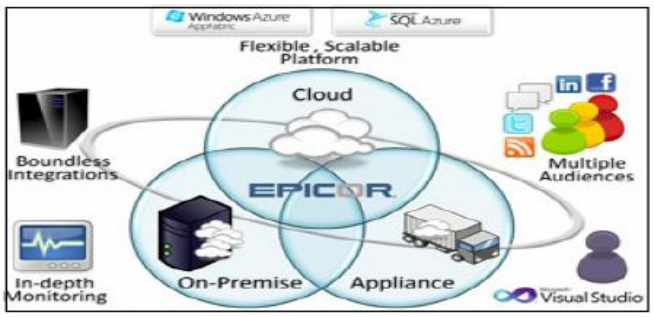

Figure 5: Elasticity

Measured Service: Tharam Dillon (2010) argue that even though computing resources are pooled and shared among multiple customers, the cloud

environment should have a better platform to evaluate the services (including software, platform, & infrastructure) delivered to customers through its flow measurement abilities. As can be seen in Fig.6, the cost of using the system's computing resources is calculated on an as-used basis.

Figure 6: Measurements

CLOUD SERVICES

The following three models have been widely employed by the cloud community to serve their customers. According to Mohamed Al Morsy (2010), Fig.7 depicts the cloud service structure for IaaS, PaaS, and SaaS.

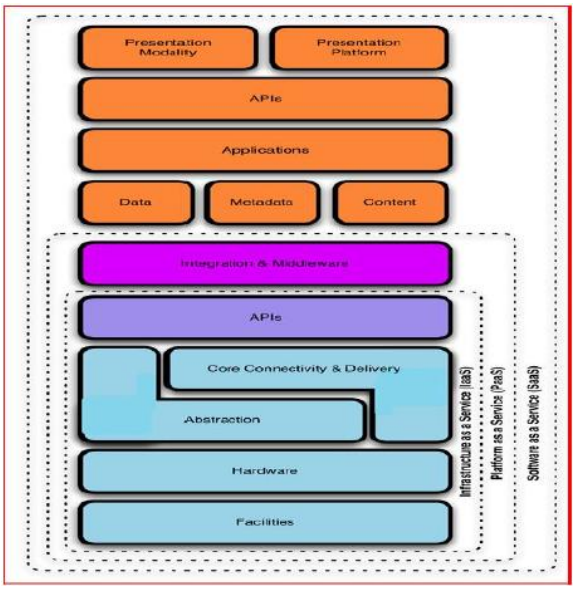

Figure 7: Service Models

(i) Software as a Service (SaaS): Customers who use cloud computing make their apps available on a hosting environment, from which end users of various devices (web browsers, PDAs, and etc) can download them. Multi-occupancy structure, systemic planning, in which different cloud shopper applications are requested in a particular context on the SaaS, cloud to recognize economies of scale & advancements in quickness, security, convenience, disaster recovery, & protection, gives up control of the cloud infrastructure to the cloud provider. Examples of software as a service included Google's email & document sharing services, as well as SalesForce.com.

(ii) Platform as a Service (PaaS): PaaS, is a development platform that partners the whole "Programming Lifecycle," enabling cloud customers to launch cloud services & applications (such as SaaS) directly on the PaaS cloud. The distinction between SaaS &PaaS is that the former only provides permanently available cloud apps, while the latter provides access to a development platform with both fully functional & ongoing cloud application projects. This necessitates that PaaS, in the group to support application hosting environment, own the development foundation including programming environment, instruments, structure administration. For instance, Google AppEngine is a PaaS.

(iii) Infrastructure as a Service (IaaS): IaaS cloud users rely heavily on information technology (IT) organizations for their services (including for storage, processing, and other crucial back-end infrastructure). IaaS clouds frequently make use of virtualization to partition their underlying hardware in a tailored manner in response to changes in asset demand from their user base. Positioning & managing VMs that are cut off from both the host machine or other VMs is the foundation of virtualization. In contrast to the multi-occupancy model, which safeguards alterations to the architecture of an application to accommodate the simultaneous execution of several events (for a variety of cloud customers), this strategy does not require any such changes (i.e. the same rationale machine).

(iv) Data Storage as a Service (DaaS): Interest-based adoption of virtualized storage evolves into a novel Cloud administration - that of data storage and management. It's possible that Data as a Service will be recognized as a key category of Infrastructure as a Service. The reason for this is that the upfront costs of a dedicated server, programming license, post-conveyance services, and in-house IT support can quickly add up when database plans become entangled on a substantial project. DaaS lets clients to wage for what they are genuinely utilizing instead of the site allows for the full database. Some DaaS moreover include table-style ideas intended to scale out to store & recover a gigantic amount of information within the accurate straightening timescale, which is commonly too extensive, too opulent, or too abating for most company RDBMS to adapt to. This category of DaaS is illustrated by services like Amazon S3, Google Big Table, Apache HBase, etc.

CLOUD DEPLOYMENT MODEL

Currently, the Cloud community has defined four distinct models for sending clouds:

(i) Private cloud: The cloud infrastructure is managed by the company itself and is either self-fulfilled or outsourced depending on whether it is an organized proof or off-purpose. There are many incentives for setting up a private cloud within an organization. The initial goal is to maximize & improve the usage of already existing resources inside the organization. Secondly, many businesses opt for Private Cloud because they are concerned about security, especially when it comes to safeguarding sensitive data. Third, the cost of sending data from a regional IT hub to the Public Cloud is relatively high. Fourth, as depicted in Fig 8, as explained by Tharam Dillon (2010), organizations always require total control over mission-differentiating activities taking place beyond their borders.

Figure 8: Private Cloud

(ii) Community cloud: When many organizations work together, they can construct & utilize a single cloud infrastructure that satisfies everyone's needs, standards, and concerns. The cloud community has reached a point of fiscal scalability & self-governing equilibrium. According to Fig 9, the cloud infrastructure may be hosted by an external provider or by the respective enterprises themselves. Tharam (2010).

Figure 9: Community Cloud

(iii) Public cloud: Tharam Dillon (2010) exemplary Cloud computing deployment model is depicted in Fig 10. All public cloud users use the public cloud, which is wholly owned by each cloud service provider with their own set of policies, values, profits, costs, & charging models. A few examples of well-known public clouds are Amazon EC2, S3, Google App Engine, & Force.com.

Figure 10: Public cloud

(iv) Hybrid cloud: Two or more clouds (private, community, or public) that function as independent units but are bound together by a common or branded technology that enables data & application portability make up the cloud organization (e.g., cloud bursting for load-balancing between clouds). Hybrid clouds allow businesses to maximize their resources and boost their core capabilities by shifting some non-essential tasks to the cloud while keeping management of their most important tasks in-house, in a private cloud. According to the descriptions provided by Tharam Dillon,(2010). Because of the hybrid cloud, previously-existing problems with calibration & cloud interoperability have become much more severe.

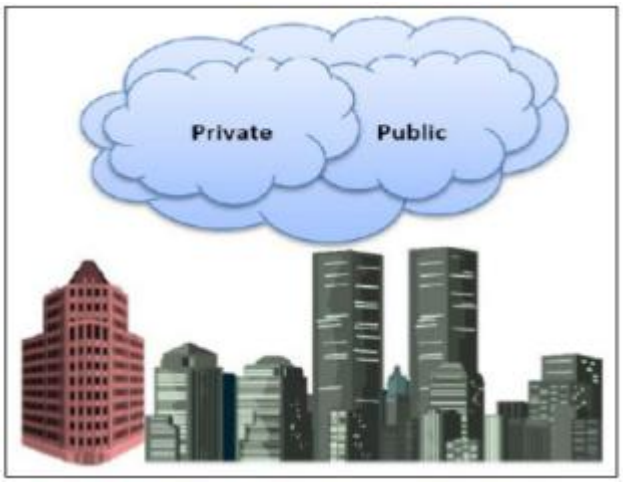

Figure 11: Hybrid Cloud

SECURITY ISSUES IN CLOUD

The importance of security measures cannot be overstated when considering various cloud service providers. Thus, security-focused cloud providers might become trusted accessories if they are able to meet the security requirements of their customers. According to Mohamed Al Morsy (2011), a cloud provider firm can expand rapidly if it provides superior ease of use and safety. It is apparent that businesses are hesitant to use cloud services because of security concerns, creating a precarious situation for cloud service providers. This learning guide discusses the primary cloud security challenges encountered by providers. They learn how to reassure prospective customers and how to capitalize on their provider's position as an industry leader in cloud security. Security concerns are perhaps the biggest roadblock in the transported processing industry. ISV (Independent Software Vendor) companies will now feel an immediate and significant negative effect on their organization's consistent quality if security flaws are discovered. Concurrently, the research given in the NIST paper emphasizes assurance & security associated challenges that are widely acknowledged to have long-term centrality for communicated registering.

Figure 12: Guidelines on Security and Privacy in Cloud Computing

i. **Administration** – The affiliation is at risk if safety & monitoring arrangements are disregarded. Establishing audit frameworks & equipment is necessary for making decisions about data security & usage, recognizing organizations, and verifying system authorization.

ii. **Consistence** – Consistency includes adhering to a protected standard, regulation, legislation, or other stipulation. Within mixed-country contexts, security & assurance laws & regulations can vary widely from country to country, state to state, and municipality to municipality, making compatibility a potentially thorny issue for distributed processing. Both the legal requirements of the customer and the acceptability of the cloud shippers should be investigated by the ISV or IT affiliate.

iii. **Trust** – The SaaS vendor gives up direct management of certain aspects of security. When deciding on a cloud provider, it is important to keep in mind that both IaaS&PaaS vendors will have access to your organization's internal network. This means that your cloud vendor's employees, managers, or other third parties will be able to see & manipulate your data. It's crucial that IaaS and PaaS cloud providers work together in harmony. Although, this does not ensure that the SaaS dealer will verify the unveiling of the strategies prior to signing on the dotted line with several cloud service providers.

iv. **Information security** – Many would-be users of SaaS are concerned about the safety of their data due to concerns about data isolation.
   a. By "data withdrawal," we mean the general impossibility, under the given conditions, for a particular patron (consumer) to review the data of other renters.
   b. When a limit is changed or defenses are maintained, data security requires a stringent method that is itself stringent.
   c. c. Data must also be encrypted & combined when at rest, in transit, or in use. Correspondence & convention models, as well as open-key confirmations & data trade licenses, can all benefit from cryptographic protections.

v. **Accessibility** - The conversation regarding availability has been ongoing & sincere since Amazon's disappointment a month ago. To guarantee the recovery of cloud organizations & operations, it is crucial to conduct a thorough investigation into the openness & resoluteness of a cloud dealer, such as its support &

recovery capabilities. Similar preparations should be made for the SaaS provider's own disaster recovery, including reaching out to industry groups, suppliers, and even the ocean floor. Planning for this must take conducted within its cloud employing cross-cloud workplaces & possibly even cross-cloud vendors.

vi. **Occurrence reaction** -A well-organized plan for handling the fallout of a cyberattack on a computer system. Activities like scene checking, attack analysis, regulation, data social occasion & preservation, problem repair, or organization reorganization are all crucial parts of event reaction, and the cloud provider plays a crucial role in each of these. The SaaS provider should take similar measures to those taken in the final region of availability to ensure the application layer is secure by implementing measures such as virtual private networks (VPNs), application surveys, antivirus software, etc.

The half-and-half cloud model is used by businesses in an effort to improve their resources & increase their core competencies by shifting some of their peripheral business functions to the cloud while maintaining control over their core activities in-house or via a private cloud. The problems of institutional & cloud interoperable have been brought to light by the rise of the crossover cloud. These will be discussed more in the next chapters.

The most fundamental barrier to Cloud computing is security concerns. Many people are intimidated by the prospect of entrusting their data to another person, launching their product on someone else's hard disk, or employing someone else's CPU. Data loss, phishing, & botnets (software that runs remotely on a network of computers) are just a few examples of the many serious information & programming security challenges that offer real risks to any organization. New security concerns have emerged due to distributed computing's multi-tenure paradigm & pooled processing assets. Fig13 displays the findings of an IDC (International Data Corporation) research on unique concerns of the cloud model raised by Chief Information Officers & Business Leaders (Chief Executive Officer). Evidence from the on-demand approach proposed by Tharam Dillon (2010) reveals that security is the primary concern.

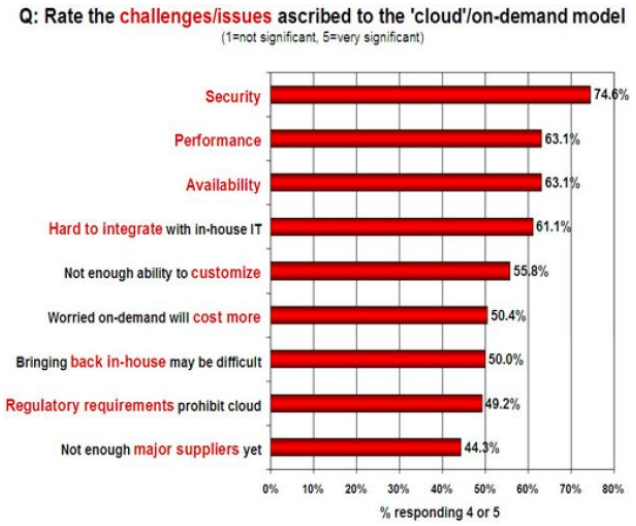

Figure 13: IDC Survey Report

At the very least, two more security concerns have arisen as a result of the multi-tenancy paradigm. First, unexpected side channels among a malicious resource & regular one can be established when those resources (hard drive, data, VM) are shared on the similar physical computer. As a second point, the problem of "reputation fate-sharing" will seriously harm the reputation of many good Cloud "citizens" who, unhappily, share the computing resources with their fellow tenant - an infamous user with a criminal mind. If multiple users on a network have the same IP address, it will be impossible to determine who is actually a subversive actor.

SECURITY MECHANISMS

There exists various security mechanisms that when applied to the cloud environment can help mitigate several of the vulnerabilities. Some of the techniques for providing data security (Harpreet*et al.* 2014) are:

Encryption: Encryption helps in converting the message into the encrypted form by making use of the various methods available. As a result anybody without the decryption key cannot decrypt and read the original message. The encryption mechanism can help counter traffic eavesdropping, malicious intermediary, insufficient authorization, and overlapping trust boundary security threats. For example, malicious service agents that attempt traffic eavesdropping are unable to decrypt messages in transit if they do not have the decryption key. Data encryption provides an effective way for protecting data confidentiality. The price of it is the degradation of efficiency and flexibility for data processing.

Message Authentication: Message authentication helps to ensure the trustworthiness of data

retrieved from the cloud. Hashing is a technique used to verify the authenticity of messages. A hash code or message digest is generated using the hash function on the message and the generated hash code or message digest is usually concatenated with the original message and sent to the receiver. The recipient applies the same hash function to the received message and generates a message digest and verifies that the produced message digest is identical to the one that accompanied the message. Any alteration to the original data results in an entirely different message digest and clearly indicates that tampering has occurred. In addition to its utilization for protecting stored data, the cloud threats that can be mitigated by the hashing mechanism include malicious intermediary and insufficient authorization.

Digital Signature: A digital signature is used to verify the authenticity of the sender and to ensure non repudiation. A digital signature generated with the message is appended to the message prior to transmission, which is then rendered invalid if the message experiences any subsequent, unauthorized modifications.

Identity and Access Management (IAM): The Identity and Access Management (IAM) mechanism encompasses the components and policies necessary to control and track user identities and access privileges for IT resources, environments, and systems. The IAM mechanism is primarily used to counter the insufficient authorization, denial of service, and overlapping trust boundaries threats

Single Sign-On (SSO): The Single Sign-On (SSO) mechanism enables a cloud service consumer to be authenticated by a security broker, which establishes a security context that persists while the cloud service consumer accesses other cloud services or cloud-based IT resources. The cloud service consumer has to re-authenticate himself with every subsequent request. This mechanism does not directly counter any of the cloud security threats. It primarily enhances the usability of cloud based environments for access and management of distributed IT resources and solutions.

CONCLUSION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction", as defined by NIST. Clouds can also be classified based upon the underlying infrastructure deployment model as Public, Private, Community, or Hybrid clouds. The different infrastructure deployment models are distinguishable with their own characteristics. The security of the IoT and cloud computing in a sustainable IoT network will have huge impacts. This incorporation will exposed to new and thrilling solutions and a route for organization and academic research. The future mixture cloud computing architecture for a human centric IoT network.

REFERENCES

1. Mohamed. A history of cloud computing. ComputerWeekly, 2009. URL http:// www:computerweekly:com/feature/A-history-of-cloud-computing. Accessed: 18-05-2015.
2. S. Raja and S. AbdRazak. Analysis of security and privacy in public cloud environment. Cloud Computing (ICCC), 2015 International Conference, pages 1{6, 2015. doi: 10:1109/CLOUDCOMP:2015:7149630.
3. Chen J, Wang Y & Wang X 2012, On-Demand Security Architecture for Cloud Computing, Computer, vol. 45, pp. 73-78.
4. Chen, D & Zhao, H 2012, „Data security and privacy protection issues in cloud computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), pp. 647-651.
5. Chen and H. Zhao. Data security and privacy protection issues in cloud computing. 2012 International Conference on Computer Science and Electronics Engineering, pages 647{651, 2012.
6. D. H. Tran, H. L. Nguyen, W. Zha, and W. K. Ng. Towards security in sharing data on cloud-based social networks. 2011 8th International Conference on Information, Communications and Signal Processing (ICICS), pages 1{5, 2011.
7. Wang C, Bi Z, Da Xu L 2014, IoT and cloud computing in automation of assembly modeling systems, IEEE Transactions on Industrial Informatics , vol. 10, no. 2, pp. 1426-1434.
8. Wei, L, Zhu, H, Cao, Z, Dong, X, Jia, W & Chen, Y 2014, „Security and privacy for storage and computation in cloud computing", Information Sciences, vol. 258, pp. 371-386.
9. Xiao, Z & Xiao, Y 2013, „Security and privacy in cloud computing", IEEE Transactions on Parallel and Distributed Systems,, vol. 15, no. 2, pp. 843-859.
10. Z. Xiao and Y. Xiao. Security and privacy in cloud computing. Communications Surveys and Tutorials, IEEE 2012 Issue 99, pages 1{17, 2012.
11. Zissis, D &Lekkas, D 2012, „Addressing cloud computing security issues", Future

Generation computer systems, vol. 28, no. 3, pp. 583-592.

Corresponding Author

Saket Nigam*

Research Scholar, Shri Krishna University, Chhatarpur M.P.