

SECURITY CONCERNS IN CLOUD COMPUTING: AN EMPIRICAL STUDY OF HIGHER EDUCATION INSTITUTIONS IN SAHARANPUR

Vinod Kumar

Research Scholar, Shobhit University, Gangoh
Email: vinod.kumar@shobhituniversity.ac.in

Dr. Mahipal Singh

Associate Professor Shobhit University, Gangoh
Email: mahipal.singh@shobhituniversity.ac.in

ABSTRACT

The word Cloud computing is the most prominent word in the contemporary world of information technology. This model has changed the entire domain of computing due to its reliability, validity, and economic nature. Over the last decade, cloud computing has given the pace to Information Technology. With this rapid growth in this sector, various security issues have been addressed and concerns regarding the security of information. With the information increment in cloud platform, security concerns are also to be considered. Due to these security concerns, there is a lack of investment inclination in this sector from the organizations.[1]. The present research paper aims to investigate the knowledge and attitude towards the security concerns in cloud computing. Methods: Qualitative analysis and quantitative survey methods have been adopted for the present research paper. Findings: The findings of the survey reveal that effective laws and policies are required for the security and privacy in cloud computing. Cloud computing has the potential for improving efficiency, cost, and convenience for the universities, especially in higher education (67.3%) (Q3); cloud computing deployment model is more suitable for higher educational institutions (52%) (Q4); In global scenario as well as in higher education institutions in Saharanpur security concerns are major barrier in cloud computing. The survey indicated that most of the respondents (70%) agreed that privacy and confidentiality are the issues which make immediate attention of lawmaker in the cloud computing (Q9).

Keywords - Cloud computing, Data privacy, Security concern

Introduction

In the world of information technology, Cloud can be defined in different ways according to the specific domains like software development or system or database administrator. Generally, Cloud means a wide-ranging measurable service that can be accessed through internet by the users. Cloud Computing is a technology in which data and programs are stored and accessed over the Internet.

In other words, "Cloud computing is a technology by which data or information is stored, managed and retrieved with the help of the Internet." Cloud computing is a mode of delivery that includes hosted services over the Internet. Cloud computing includes a variety of resources such as data storage, servers, databases, networking, and applications. Whenever we store any data in the computer, we store it in the hard disk, but through cloud computing, we can store

our data in the cloud. Hard disks, databases and software applications are used to develop cloud computing.

Cloud Computing: An architectural view

Cloud computing is a very popular technology for any business or firm because it reduces costs, increases productivity, improves security, and enhances performance. This is a better option for those organizations that require more memory space and must take backups from time to time. The services in this technology can be both private and public. These services are divided into three categories, the first IaaS, the second PaaS and the third SaaS.

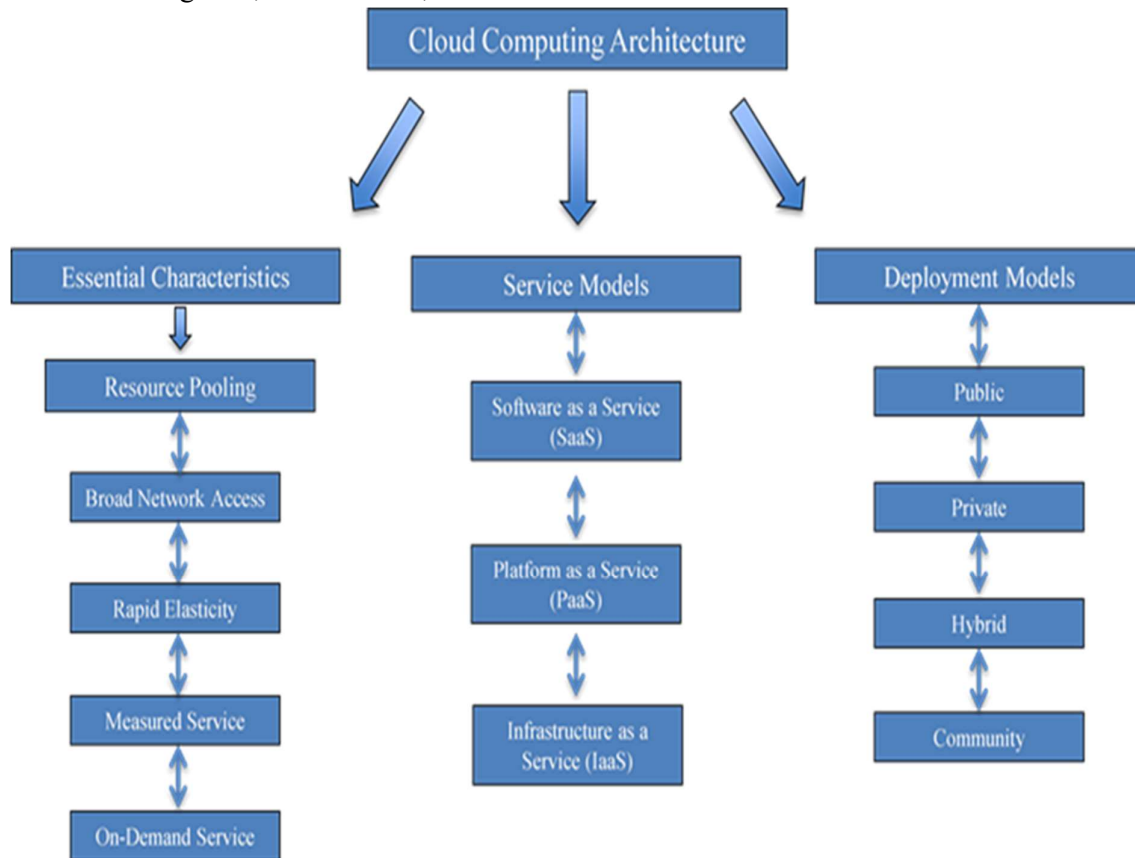


Figure 1: A general overview of cloud model

Major Security Issues in clouding computing

The models have a lot of negatives in terms of security concerns and problems with cloud computing systems since they also provide information that increases those risks and problems. The very first layer IaaS, which is the base of the functionalities of entire cloud, is easily approachable to the hackers. Other security issue of cloud models is data damage. Data accessibility is a big challenge in cloud models as internally unauthorized persons from any organizations access data and external hackers can access of database through hacking tricks, Trojan and Viruses. [2] To develop a system with stronger security procedures to safeguard cloud computing environments, it is critical to identify potential cloud risks.

Various Threats in cloud computing

1.1 Credentials Access and authentication problem

Employee engagement and job switching is a major problem within organizations in current scenario that affects the user's authentication. More than 80 million customer details were exposed in the Anthem breach, which was caused by stolen user passwords. Since Anthem didn't use multifactor authentication, everything was lost once the attackers got their hands on the credentials. Numerous developers have made the error of storing credentials and cryptographic keys in public-facing repositories and embedding them in source code. [3].

2. Security challenges in Service model

2.1 Miscellaneous attacks

Both internal and external sources can provide security risks to businesses. 21% of cyber-attacks, according to the 2011 Cyber Security Watch Study, were initiated by insiders. According to 33% of respondents, internal threats are more expensive and harmful to organizations. The majority of insider assaults (63%) and intellectual property theft (32%), respectively, involved unlawful access to and use of corporate information. Some sensitive data can be accessed by malicious users, which can result in data breaches. Farad Sabah has revealed malicious attacks by unauthorized users on the IP address and physical server of the victim. The malicious intent could be anything from data theft to retribution. An insider in a cloud environment has the authority to alter, steal, or destroy entire infrastructures. The most vulnerable systems are the ones whose security is totally dependent on the cloud service provider [4]

2.2 Backup and storage

The cloud provider should make sure that regular data backups are implemented, and that security is fully protected. However, the backup data is typically located in an unencrypted format, which might result in data misuse by unwanted parties. Data backups subsequently present a number of security risks. An exceedingly challenging backup and storage issue arises as server virtualization grows. [5].

2.3 Service hijacking

Service hijacking refers to unauthorized users taking illegal control of specific allowed services. It may be accomplished using a number of strategies, including fraud, phishing, and software exploitation. One of the threats is this. One of the greatest threats has been identified as account theft. [6].

Security challenges in Deployment model

3.1 PaaS security issues

PaaS enables the deployment of cloud-based applications without incurring additional costs for the purchase and upkeep of the supporting hardware and software layers.[7] A safe and dependable network is necessary for PaaS. Security for customer applications installed on a PaaS platform and security for the PaaS platform itself make up the two software layers that make up PaaS application security.

3.2 Third party relations issues

PaaS provides third-party web services components like mashups in addition to standard programming languages. Mashups can incorporate multiple source elements into a single, cohesive whole.[8] As a result, security problems with mashups affect PaaS architectures.

Users of PaaS are reliant on the security of both third-party services and web-hosted development tools.

3.3 Cloning

Cloning is the process of reproducing or replicating data. Data leakage issues brought on by cloning can expose the machine's legitimacy. Wayne A. Pauley contrasts this by stating that resource pooling is a service offered to customers by the provider that enables them to access various resources and share them in accordance with application demand.[9] Unauthorized access resulting from sharing across the same network is known as resource pooling. Researchers' studies on virtual and cloud computing show that a virtual machine can be provisioned very quickly, as well as reversed to prior situations, paused and easily restarted, and moved between two servers, posing non-auditable security risks.

3.4 Unencrypted data

Data encryption is a procedure that aids in removing different harmful external threats. Data that is not encrypted is extremely susceptible to attack since it lacks any security measures. Unauthorized individuals can very simply access unencrypted data. Unencrypted data exposes user information to danger, which allows unauthorised users to access diverse data from cloud servers [10]. For instance, the well-known file-sharing service Drop box was charged with storing all user data using a single encryption key. Malicious people are encouraged to misuse the data in one way or another by these unprotected, insecure data.

3.5 Flooding attacks

In this kind of assault, the intruder makes a lot of resource requests to the cloud quickly, flooding it with a lot of demands. According to a study done by IBM [11], the cloud has the ability to grow depending on the volume of requests. It will develop so that it satisfies the demands of the invader, rendering the resources unavailable to regular users.

Cloud Computing in Higher Education:

Higher education is one of the essential pillars of the social development. Universities, government, and industry have contributed to the world economy and transformation of society. Along with internet resources, the educational institutions use cloud computing for data analysis and data storage. In the education field, cloud computing is practical for different types of reasons. The educational system has suffered from lack of resources like staffing cuts, small classrooms, and lack of qualified teachers. For the enhancement and facilitation of higher education cloud computing is much required tool. These challenges will be managed in a different number of ways by using cloud computing. The problem of overcrowded classrooms will be determined by virtualizing the classroom environment 14. Students can attend the classes of the classroom environment by logging into the online platform. The instructor does not need to know the way to deal with classes. They can only focus on developing contents for the students and build the student skills and help them pass the exams. Cloud allows the students to share the education infrastructure, ideas, and tools that result in effectively reducing the cost for the educational institution. The availability of quality learning materials like software and books, which can be equally accessed by everyone in the cloud environment can help the students in improving their academic performances thereby enhancing the ability of the institution, which otherwise has insufficient physical resources, in providing quality education. Cloud computing's SaaS model has become popular in the higher education. The

adoption of cloud computing is in the initial stage in Saharanpur. Many surveys have been conducted to encourage the country to use the cloud in the organization. Saharanpur is at the stage of worrying factors as there is a need for more investment in building up the data centre with servers and the storage capacity for the use of the IT application. At the same time, Uttar Pradesh would have increased the productivity of the resources, scalability, and cost reduction for the implementation of the applications in the cloud. The third party of the cloud that reduces the responsibility and cost of the organization do the maintenance of the IT resources and the production. The cloud computing enhances the education system by providing quality services to the students.

Research Methodology

The study applied a qualitative and quantitative method throughout the discussion and analysis on current issues in Cloud Computing in educational sectors in the Saharanpur district of Uttar Pradesh. The qualitative research focused on the reviews of past research in the field of cloud computing while for quantitative results a questionnaire-based survey was conducted for finding the risks and challenges involved in the use of cloud computing in higher education in Saharanpur. The responses from the survey were then analysed quantitatively by statistical analysis to draw conclusion. Questionnaires were distributed to two types of people in the educational sectors, namely to Faculty and to IT Staff in Saharanpur. The objectives of the survey were to highlight the challenges and barriers in adopting cloud computing and evaluate the privacy, security issues and existing legislation practiced for data protection and privacy. The survey consists of closed-ended questions. A total of 100 people participated in the survey. The respondents were contacted in person and through e-mail.

Statistical Analysis

All the collected data were subjected to statistical analysis. Association between various categorical data was analysed using Chi-square statistics. A p value ≤ 0.05 was considered statistically significant.

Theoretical Framework

Here, an integrated theoretical framework for adoption of cloud computing by educational institutions in Saharanpur is proposed through analysis of perceptions of different types of staff (Faculty and IT staff) of different age group of males and females from ten different higher education Institutions in Saharanpur. The survey tried to find the benefits of cloud computing in educational sector in Saharanpur and factors affecting its adoption in the educational sector. In this framework, the factors of and the barriers to cloud computing adoption are categorized into three contexts such as technology, organization, and environment. Since the survey is conducted among faculty and IT staff who are at the forefront of any such change in technology, we believe that their perception and analysis will provide more realistic insights into barriers in adoption of cloud computing in educational sectors in Saharanpur.

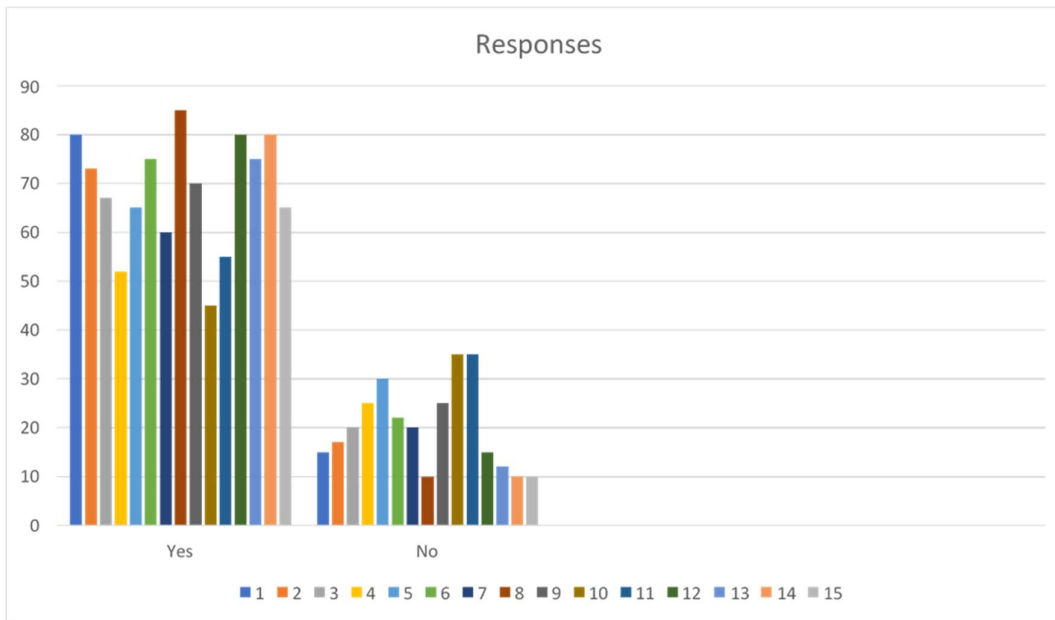
The survey questionnaire was distributed among the educational institutions. The questions were related to familiarity with cloud computing and their risks related to security, confidentiality, and privacy. There were 50% faculty and 50% IT staff. Most of the participants (62%) were in the age group of 35 – 40 years. The number of participants from each of the ten institutions was comparable and varied between 14-20%. Table 1 shows the characteristics of

the study population that participated in the questionnaire survey. The responses to the survey questionnaire are summarized in Table 2

Table 1
Characteristics of the study population

Variables		N
Staff Type	Faculty	50
	IT Staff	50
Age (Years)	20-25	5(5.0)
	25-30	15 (15.0)
	30-35	18 (18.0)
	35-40	62 (62.0)
Gender	Male	45
	Female	55
Institutions	Shobhit University, Saharanpur	
	Hari Institute Technology, Saharanpur	
	Ramdoot College Nakur Saharanpur	
	Satguru Institute Technology, Nakur, Saharanpur	
	Maa Shakumabri University Saharanpur	
	Dev Bhoomi Institute of Technology	
	Puranmal Ramlal degree College Gangoh Saharanpur	
	Gochar Mahavidhalya Rampur	
	Indraprastha Institute Kota Saharanpur	
	IPS Institute Gangoh Saharanpur	

Table 2
Graphic representation of Responses (Question wise)



Conclusion

Cloud Computing is a new paradigm in the field of computer science that has changed the user experience in many beneficial ways, but various security issue has arisen with its development. Vulnerabilities that exist in the model of Cloud Computing is a major issue in its organizational modality. Although Cloud Computing empowers many technologies but rather it leads towards many security questions. The present research paper presented security issues for cloud models: IaaS, PaaS, and SaaS, which differ depending on the model. Various reviews describe that in cloud computing, storage, and networks along with the authentication problem, Data encryption and browser security are the biggest security concerns. Server sharing (virtualization) is also a foremost security concern for cloud users. The findings of the survey indicated that most of the respondents (85%) agreed security risk is the significant challenge which acts as a barrier for computing educational services in Saharanpur (Q8). 15% of the respondents stated that they are not aware of the usage of cloud services and technologies. About 80% believe that most of them are familiar with and using (Q1). Majority of them believe that cloud computing is an emerging concept which is helpful in higher education institutions and universities (73%) (Q2); cloud computing has the potential for improving efficiency, cost, and convenience for the universities, especially in higher education (67.3%) (Q3); cloud computing deployment model is more suitable for higher educational institutions (52%) (Q4); and cloud computing will bring drastic changes in educational institutions (65%) (Q5). Most of the survey respondents strongly agreed that cloud computing is the effective technology in education and enhance student’s technical skills and also make them lead a contemporary life. Total 75% respondents believe that cloud Computing reduce the operational and maintenance cost of the universities (Q6) and 60% believe that cloud computing provides universities a centralized, virtual data centre that is accessible to faculty and admissions personnel (Q7). The survey indicated that most of the respondents (70%) agreed that privacy and confidentiality are the issues which make immediate attention of lawmaker in the cloud computing (Q9).

References

- [1] B. R. Kandukuri, V. R. Paturi and A. Rakshit, "Cloud Security Issues," Proceedings of the 2009 IEEE International Conference on Services Computing, Washington DC, 21-25 September 2009, pp. 517-520.
- [2] D. Jamil and H. Zaki, "Security Issues in Cloud Computing and Countermeasures," International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676.
<http://www.infoworld.com/article/3041078>
- [3] Jathanna, Rohan & Jagli, Dhanamma. (2017). Cloud Computing and Security Issues. International Journal of Engineering Research and Applications. 07. 31-38. 10.9790/9622-0706053138.
- [4] Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486-2, IEEE, 2011, pp: 245 – 249
- [5] Jathanna, Rohan & Jagli, Dhanamma. (2017). Cloud Computing and Security Issues. International Journal of Engineering Research and Applications. 07. 31-38. 10.9790/9622-0706053138.
- [6] Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee, "A Survey on Cloud Computing Security, Challenges and Threats", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol. 3 No. 3 March 2011, pp: 1227 – 1231.
- [7] Subashini S, Kavitha V: A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 2011, 34(1):1–11. 10.1016/j.jnca.2010.07.006
- [8] Mather T, Kumaraswamy S, Latif S: Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.; 2009.
- [9] Wayne A. Pauley, "Cloud Provider Transparency – An empirical evaluation", the IEEE computer and reliability societies, IEEE, November 2010, pp: 32 – 39
- [10] Cong Wang, Ning Cao, Kui Ren, Wenjing Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE transactions on parallel and distributed systems, IEEE, Digital Object Identifier 10.1109/TPDS.2011.282, 2011, pp: 1 – 14
- [11] Web 2.0/SaaS Security, Tokyo Research Laboratory, IBM Research. http://www.trl.ibm.com/projects/web20sec/web20sec_e.htm