Cloud Computing Security Challenges in Higher Educational Institutions - A Survey

Khalil H. A. Al-Shqeerat
College of Computer
Qassim University
Qassim - Saudi Arabia

Faiz M. A. Al-Shrouf
Faculty of Information Technology
Middle East University
Amman - Jordan

Mohammad R. Hassan
Faculty of Information Technology
Al-Ahliyya Amman University
Amman - Jordan

Hassen Fajraoui
Professional Training Center PTC
"Des Riverains"
Répentigny – Canada

ABSTRACT
Cloud computing brings for higher educational institution a wide range of benefits with new capabilities to incorporate in the educational process. However, the cloud services are vulnerable to a variety of security challenges.

One of the key challenges that educational institutions face in adopting cloud computing technologies is a provisioning of a secure cloud infrastructure.

In this paper, the authors discover some cloud benefits in the education sector and discuss limitations of main cloud services as well as highlight security challenges that institutions face when utilizing cloud technologies.

The survey was conducted in variety educational institutions to study the views of stakeholders on the cloud security vulnerabilities and approaches used to overcome.

Finally, this paper provides baseline recommendations to avoid security risks efficiently when adopting cloud computing in institutions of higher education.

General Terms
Cloud Computing, Higher Education, Security, Survey

Keywords
Cloud Services, Deployment models, Benefits, Challenges, Risks

1. INTRODUCTION
Cloud computing plays an important role in improving the quality of education to achieve required performance by offering many benefits for education such as providing low-cost infrastructure, flexibility, scalability, collaboration, and ease-of-use. Furthermore, it allows users to store their critical information and access it on-demand from anywhere via the internet [1]. The cloud services and applications enable users to store and access their local data in the remote data center by using their personal computers, or mobile devices [2].

In higher educational institutions, the stakeholder term refers to anyone who has access to educational services, including students, lecturers, researchers, staff members, etc. Figure 1 shows the main stakeholders of cloud computing in higher educational institutions.

1.1 Cloud Deployment Models
Cloud computing deployment models were defined by the National Institute of Standards and Technology (NIST) and classified into four common modes; private, public, hybrid and community clouds [3].

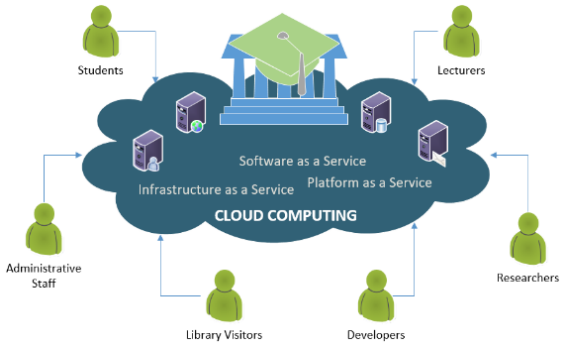

Fig. 1: Stakeholders of cloud in an educational institution.

Private cloud is deployed inside the boundary of the organization and is provisioned for exclusive use by specific consumers, its data and services cannot be accessed from outside of an organization.

Public cloud is owned and managed by a business, academic, or government organizations that provide cloud services for open use to the public.

The hybrid cloud is a composition of both public and private clouds characteristics.

In the community cloud, the infrastructure and services are provisioned for use by the specific community of consumers or among several organizations that have same mission or target. It can be operated and managed internally in the community or by a third party.

1.2 Cloud Computing Characteristics
According to the NIST definition, the cloud computing services entail about five essential characteristics; on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Here, we will discuss in details the fundamental education-based characteristics of cloud computing:

On-demand self-**service:** The diversity of users in educational institutions leads to a variety of functionality and

performed operations. In this case, the stakeholder requires freedom to provision cloud services or resources that they wish to use whenever needed without requiring direct interaction with the service provider. Usually, the user online configures and manages resources under on-demand environment through a web-based self-service interface.

Broad network access: The cloud services and resources must be widely accessible from anywhere by heterogeneous platforms such as laptops, tablets, mobile phones, etc. This ubiquitous access is established using standard access mechanisms and protocol. To enable this level of access in educational sectors requires that services be tailored according to demands of different cloud users.

Resource Pooling: The cloud providers pool large-scale computing resources and services to serve multiple users separately on a logical level. This multi-tenant model relies on virtualization technology where resources are dynamically assigned and re-assigned according to cloud user demand. A multi-tenant environment is promoting location-independence whereby the user has no knowledge where data is being located or stored.

Rapid elasticity: The cloud services or resources provisioned to the user can be scaled up and down rapidly based on the user policy and requirements, with no impact on the application or any human interaction. In this case, different stakeholders in an institution like students, faculties, and administrative staff can access and employ resources as needed with exact capacity and at any time.

Measured services: The usage of cloud services or resources must be monitored, metered permanently by a performance with the pay-per-use feature. This report about resources usage is provided transparency for both the service provider and user.

Resiliency: Resilient computing is the ability to recover failure and disaster of cloud resources by using multiple redundant implementations of cloud services across physical locations. Multiple redundant sites support continuity and improve the reliability and performance of cloud computing processing. If any of cloud resources becomes deficient, other redundant resources are implemented automatically.

Cost effectiveness: The cloud services and resources are cost effective as compared to local infrastructure. Its costs are shared between multiple users from same or different locations.

1.3 Cloud Service Models

In general, three main types of services the user in the educational institution can gain when access cloud. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [4]. These services are built on the cloud upon each other as shown in figure 2.

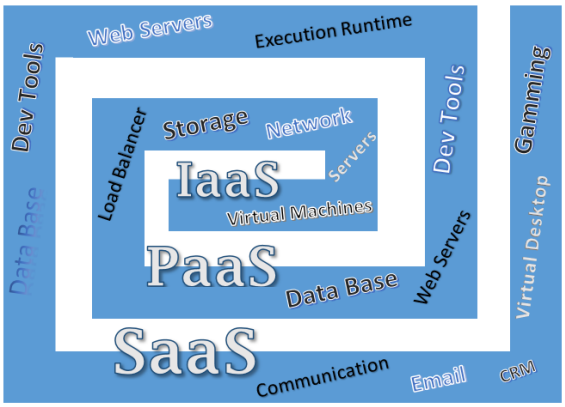

Fig. 2: Cloud service models.

In the SaaS model, users gain access anytime and from anywhere to applications provided and managed by the service provider. Currently, SaaS is considered the most interested for stockholders in education. Google Drive, Twitter, Dropbox, YouTube, and OneDrive are general examples of cloud-based services. Both Microsoft and Google provide some services that are suited for education such as Live@edu and Google Apps.

In PaaS, the service provider offers for developers development tools to build or customize their applications or services in the cloud independent of the platform to run. The best-known example of PaaS is the Google App Engine where a developer can install and customize their applications using Python language.

IaaS is a self-service model, the cloud vendor allows developers to access, monitor and manage computing resources (processors, storage, networks, etc.) in the data center remotely, and use them to run own operating systems and applications. The big advantage of using IaaS is that it offers an on-demand data center without requiring you to purchase or install new expensive equipment. Amazon's Elastic Compute Cloud is one common example of IaaS.

1.4 Cloud Benefits in Educational Institutions

There are various advantages may be granted when adopting cloud computing technologies in higher education institutions. Some universities have adopted cloud computing in their programs for economic purposes, while other institutions use the cloud to provide scalable and flexible IT services [5].

The key benefits of cloud computing in education can be categorized according to stakeholders who use cloud resources and services in higher education institutions:

1.4.1 Benefits for students:

The first beneficiary of the cloud technology in the educational institutions must be students [6]. Some of the cloud benefits directed to students are reviewed:

- Cloud computing releases services for students with new capabilities that were not served well by traditional ways. Nowadays, the students can store anything electronically such as their schedule, class notes, reports and any other documents. Furthermore, they able to back up their files to the cloud and retrieve them when needed.
- Students can earn e-copy of textbooks and have access to quality learning materials of their courses. This solves the problem of the student's reluctance

to gain textbooks due to their high-cost prices. Furthermore, cloud-based textbooks solve the problem of using outdated materials in many of institutions and allow students to access the most updated learning resources.

- The lab's applications and auxiliary resources that may be implemented on the Internet enable students to perform lab's tasks from anywhere and by low-cost personal devices. Therefore, the students do not need anymore to buy expensive hardware or install special software.
- Students have the opportunity to access the system easily at any time to get courses online, attend the online exam, and upload their assignments and projects through the cloud to the instructors.
- Real time collaboration between students themselves as a team or between students and their instructors on the other hand.

1.4.2 Benefits for faculty

The faculty also can get various advantages over cloud-based applications [7]:

- Cloud technology offers for instructors an easy and flexible platform to prepare their course tutorials, presentations, conferences, articles, etc.
- The faculty may be able to exchange experiences by establishing remote seminars to overcome the lack of skills among some faculty members.
- Providing opportunities for instructors to work from home and use their own devices to finish assignments, prepare on-line tests, grading, and scheduling.
- Collaboration with other instructors and sharing educational resources to avoid conflict and duplication of effort.
- Getting feedback from students about the educational process.
- Cloud provides for researchers a discussion area and accessibility to global computing resources and sufficient storage capacity.

Even though the great benefits of using cloud computing in educational institutions, there are some challenges that hinder the wide scale adoption of this technology in various sectors of the university. In the current circumstances, it is not easy to track the variety security issues in cloud computing environments.

The security issues are related mainly to three key requirements: confidentiality, integrity, and availability.

The confidentiality is defined as a set of rules that prevent unauthorized user from accessing sensitive information, while integrity is a way to protect data from being modified by unauthorized user and ensure that data are retrieved accurately and trustworthy, and the availability concerned with enabling authorized users to access data reliably when needed, especially during difficult circumstances and emergencies [8].

This study aims to address the key security challenges of adopting cloud computing in higher education institutions.

The rest of the paper is organized as follows. The literature review is mentioned in the next section. Section III presents an overview of the security issues in the cloud service models. In section IV, the security challenges and risks are discussed. The survey results and discussion are presented in section V. Finally, section VI provides helpful recommendations to avoid security challenges efficiently for adopting cloud computing in higher educational institutions.

2. LITERATURES REVIEW

The security challenges and privacy issues are one of the main topics that recently researchers focus on for adopting cloud computing in education.

The [9] explored the benefits of the cloud computing in educational institutions and advantages provided by the cloud.

The authors in [10] address the general security issues related to the core technologies used in cloud computing, such as APIs, virtualization, Internet protocols, etc. in addition to discussing some cloud-specific issues which are introduced with the advent of cloud computing.

In [11], software engineering and information systems design approaches was adopted to identify the generic principles of a cloud environment and control relevant vulnerabilities and threats.

The authors in [12] proposed a framework aims to treat the security issues by establishing a relationship among the cloud service providers in which the data about possible threats can be generated based on the previous attacks on other providers. While [13] focuses on the lack of security considerations in Service Level Agreements and main security threats and vulnerabilities. The framework was developed based on collected information from security experts, practitioners, service providers and their clients.

The systematic literature review and interviews with experts have been conducted in [14] to study security issues and challenges and identify gaps between the researchers' interests and what practitioners deem important.

The authors in [15] paper reviewed the literature on challenges of adoption cloud computing in institutions and universities. The authors proposed an integrated reference model based on the challenges in the literature integrated with Technology Acceptance Model (TAM) to investigate the factors influence the users' attitudes and behaviours toward using cloud education services in universities.

In [16] authors studied the challenges towards public cloud and possibility of replacing it with private cloud. In addition, they have described how to set up a private cloud in an educational institution and prove how private cloud solutions may increase the utilization of resources, minimize risks, and improve data security.

A methodological and theoretical study is presented in [17] to seek the views of key stakeholders on the issue of cloud information security within higher educational institutions in South African. The authors demonstrate the importance of trust as a cloud computing adoption factor. A trust-centric conceptual framework is proposed for understanding and evaluating cloud computing adoption in Higher Education contexts.

In [18] the questionnaire was conducted to explore the views of students towards cloud applications and services utilized in education.

Factors that have an effect on the cloud adoption by higher education were identified in [19]. Significant factors were

found in this context are; relative advantage, complexity, and data concern.

In [20], the authors have described the demand for understanding the impact of cloud computing in computer science higher education. A number of education strategies including key knowledge areas have been identified for teaching cloud computing.

The authors in [21] have identified three critical computing education categories and described the solutions towards some challenging issues.

A SWOT analysis of the impact of the cloud computing on higher education methodologies has demonstrated in [22]. A SWOT analysis provides a helpful guide for higher education institutions when considering the migration to cloud-based systems.

In [23], a five-phase strategy has been presented for adapting cloud computing in higher education. The authors have proposed a cloud computing architecture for higher education institutions containing the various deployment models, service models and user domain.

3. LIMITATIONS IN CLOUD SERVICE MODELS

This section focuses on some limitations related to cloud service models that disserve adopting cloud computing in higher educational institutions [24], [25], [26], [27].

3.1 Limitations in SaaS

Two key limitations may effect on deploying applications under SaaS model: data locality, and integrity. Generally, the user does not know where the service provider stores data and how can be assured that no one can modify it. The lack of trust between cloud user and provider is a critical issue that should be addressed when using SaaS.

As a result, to avoid data leakage in the educational institutions the computer center in the university may host the SaaS application on its own private server or deploy it on infrastructure services provided by trusted third-party provider such as Amazon, Google, etc. For these reasons, most of higher educational institutions involved in this survey are using a private cloud, rather than public or hybrid cloud as shown in figure 3.

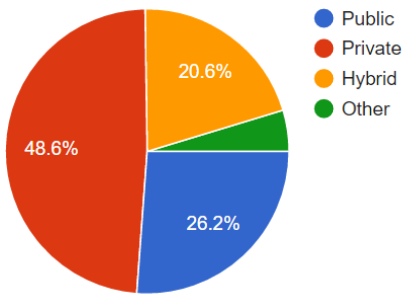

Fig. 3: Cloud models deployed in surveyed institutions

3.2 Limitations in PaaS

Although PaaS platforms provide flexibility for developers in educational institutions to accelerate development of new SaaS applications and migrate them to the cloud. However, the developers might face some challenges when using PaaS platforms.

First, the cost is increased due to adding some new features enable developers to add and control own cloud-based applications.

Another serious problem that faces PaaS users is lock-in programming models and high-level services with the vendor who provides service. These models and services are depending on particular environment and need to be completely rewritten when migrating to another PaaS environment. This less portability reduces user's freedom to migrate to another platform.

On the other hand, despite the fact that developers are able to build and control their applications on top of the platform, but they don't know any think about security below the platform which still is assigned by the service provider.

3.3 Limitations in IaaS

Compared with first two service models, IaaS provides for user better control on security issues. The main factor should be considered the reliability of stored data in the provider's resources.

The duty of IaaS model security is divided between service providers and their customers. The provider's responsibility involves main security controls such as physical and virtual environmental security. In turn, the cloud user is responsible for applying the suit security controls associated with software including operating system, developed applications and data.

Virtualization technology is a fundamental of IaaS model. In a virtualization environment, when users are utilizing the shared infrastructure resources, this may lead to a cross-tenant attack. In this case, the attacker gains root-level access and then penetrates most of the tenants' accounts in the cloud.

4. SECURITY CHALLENGES AND RISKS

Organizers in education sector are wishing to use cloud services that are not radically different from those services that totally managed within their own centers. However, they are in fact facing a range of substantial new challenges.

This section addresses the critical security and privacy-related challenges and risks in cloud computing.

To understand and successfully address the cloud security issues and its challenges in higher educational institutions, we need to investigate various aspects of cloud challenges such as threats, risks, and attack models.

Challenges in cloud computing are categorized into four main aspects; Network, Access control, Cloud infrastructure, and Data Security [28], [29], [30].

4.1 Network Security

In this category, we are discussing security-related issues of a transmission medium through which the user can connect to cloud infrastructure. Provisioning secure medium prevents leakage of sensitive information during transmission.

The most security challenges are associated with the network used as long as cloud-computing operations are totally depending on networks by which the users migrate their data to cloud servers.

As data are stored at the remote cloud server, the service provider has to provide for users a protection ways to keep data in safe from a traditional network-based attack such as DoS, Man-in-the-Middle attack, IP spoofing, packet sniffing, port scanning, etc. Table 1 below describes most of the possible attacks threaten cloud computing services.

Table 1. Traditional threats on cloud computing

Threats	Risk Description
DoS	In Denial-of-Service attack, the attacker flooding the server with traffic in order to make services or resources unavailable to cloud users.
DDoS	A Distributed Denial of Service attack is an attempt to make services unavailable by overwhelming it with traffic from multiple machines that are distributed across the Internet.
MitM	A Man-in-the-Middle attack is a type of eavesdropping attack where an intruder inserts himself into a conversation between two parties, intercepts sensitive information from users, and then passes it to the third party.
IP Spoofing	IP Spoofing is a way to gain unauthorized access to the server, whereby an attacker illegally impersonates an IP address of trusted host to conceal his identity.
Packet Sniffing	Packet sniffer or analyzer is commonly used to diagnose network-related problems. However, an attacker to capture and analyze all transmitted sensitive information can also use it.
Port Scanning	Attacker sends queries to search for vulnerable ports on the server and attempts to identify kind of used service.
Session Hijacking	An attacker can hijack an active session and masquerade as one of the conversation parties.
Phishing	Phishing is the attempt to steal sensitive user data such as usernames, passwords, and credit card details. It occurs when an attacker, impersonate an identity of a trusted entity and fools a victim to open an email, or reading an instant message.

With regard to the risks of network security in a cloud environment, hacking and intrusion are increased. This requires the use of strong network security techniques such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. Furthermore, adequate rules in firewall router, auditable access rights, and some security policies must be implemented to secure system and avoid service hijacking.

4.2 Access Control

Access Control includes important security issues such as authentication, identification, and authorization.

Since authorized users have access to the cloud via Internet, this increases security risks in cloud computing. The insecure interface of the web application is vulnerable to expose an educational institution to unauthorized access. Furthermore, weak authentication mechanism might increase the possibility of an unauthorized access to data or services which are globally accessible and shared with other users through the multi-tenancy cloud.

For this reason, using strong authentication mechanism is a basic and mandatory requirement for any cloud system to ensure the privacy of user information and data stored on a cloud provider's server.

The primary responsibility of the service provider is to protect cloud service and user data against unauthorized access. In current best practices, some good security solutions are recommended to avoid penetration such as VPNs technology, Privileged Access Management, Next Generation Firewalls, etc.

4.3 Cloud Infrastructure

This category entails issues related to the physical equipment used as a backbone for cloud infrastructure as well as the virtual software used to operate cloud resources.

The cloud infrastructure involves main features of cloud service models and is particularly associated with virtualization environment. Virtualization is a fundamental technology used by cloud vendors to achieve multi-tenant architecture, where it divides the computing resources of cloud server into multiple execution environments [31].

The virtualization-based cloud is not safe due to multi-user shared environment, where all virtual instances are on the same physical machine.

One of the virtualization security challenges faces cloud system is a lack of VM protection, because multiple VMs located on the same computer, you cannot put a hardware protection device such as a firewall between them. Another challenge is due to a dynamic environment where VMs are created, terminated, or moved to another place automatically, which make very hard to monitor traffic and determine if the attack is accruing [32].

Common attacks that might threaten cloud infrastructure are Theft-of-Service, DoS, Malware Injection, Cross-VM Side Channel, Phishing, Botnets, and VM rollback attack.

4.4 Data Security

Data Security risks constitute the biggest challenge for adopting cloud computing in higher education institution. Some institutions still prefer to store their critical data into own repositories instead of moving them to a remote cloud.

The cloud service providers have to prove to customers their ability to deal with various challenges related to data security.

Several security issues have been identified and classified according to data states in the cloud: Data-at-Rest and Data-in-Transit [33]. Data at rest refers to the data stored in the cloud servers, which need to be protected and to validate that an unauthorized user has not altered the data stored in the cloud. Especially, when data stored far away with no physical control over it such as in public cloud.

In the state of Data-in-Transit, the possibility of data loss or leakage occurring is increased when travelling from one location to another.

The major risk might face data security is the use of inappropriate encryption protocol and weak key in the cloud environment.

5. SURVEY RESULTS & DISCUSSION

In this section, we review and discuss the results obtained through the questionnaire conducted in variety universities that have adopted cloud computing. This data collection method is used to identify the point of view of stakeholders at universities on the cloud security vulnerabilities and

approaches used to overcome. Faculty members, Master students, and IT staff completed the questionnaire. Around 64% of universities covered by the survey are cloud beneficiary, whereas only 36% of them are cloud service provider.

We have noticed when reviewing the questionnaire responses that many of the respondents are not familiar with security risks that threaten their cloud or security mechanisms used to avoid. This indicates that those who responsible for cloud computing do not educate stakeholders about security issues related to their cloud computing.

The security-related survey consists of the following multiple-choice questions:

Q1. Which are the currently identified challenges regarding privacy and confidentiality in your cloud computing?

The responses on this question are distributed as shown in figure 4. The result shows 22.4 % of respondents see that security issues related to virtualization represent a challenge to cloud computing, whereas 20.6% think that encryption method used in the cloud may be a real challenge. While a lower number of respondents have selected data outsourcing (14%) and legal issues (11.2%) as challenges for cloud computing in their universities.

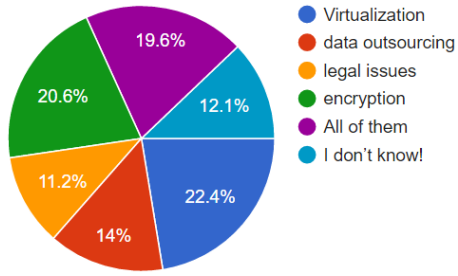

Fig. 4: Privacy and confidentiality challenges.

Q2. What are the common vulnerabilities that your cloud environment suffers from?

On this question, one-third of participants didn't have enough information about cloud computing architecture and vulnerabilities that might threaten their network, as shown in figure 5, while the rest of responses were distributed among the specified common vulnerabilities as follow; weak authentication and authorization services (17.8%), poor key management and control (15%), and other vulnerabilities that selected in the same proportions.

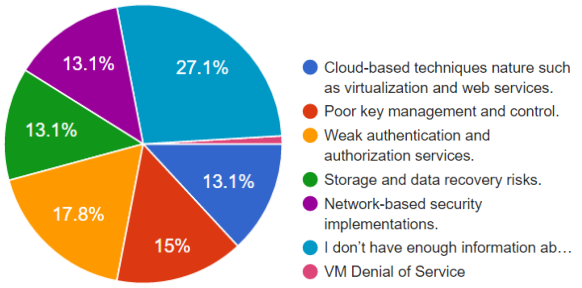

Fig. 5: Common vulnerabilities cloud environment.

Q3. Specify which of the following attacks threaten your cloud computing?

This question allows the participant in the questionnaire to select multiple answers for determining which threats or attacks might threaten their cloud platforms.

The result is shown in figure 6. The most serious security attack on cloud according to stakeholders' perspective is Denial of Service DoS (43.9%), then phishing (34.6%), and Theft of Service (30.8%).

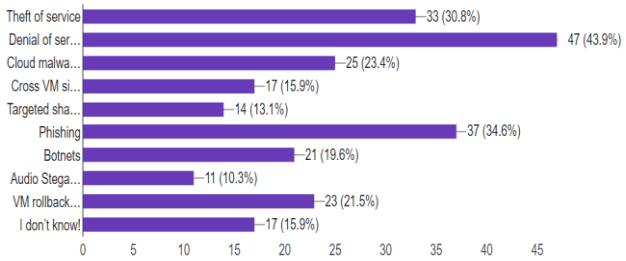

Fig. 6: Cloud threats in surveyed universities.

Q4. Select approaches that have been introduced by your institution to ensure security in cloud computing.

The figure below shows the distribution of protection mechanisms and approaches adopted by surveyed universities in order to protect data and cloud services.

The encryption and hash calculation methods are the most common solutions (25%) to assure the cloud security. Another suggested schemes such as secure framework (16.8%), proposed algorithm from literature (14%), recommended guidelines (13.1%), in addition to physical solutions like network isolation and firewalls. Finally, as was mentioned before, unfortunately, more than 25% participants in the questionnaire are not familiar with security approached and methods used in their universities to protect cloud and prevent any expected attack.

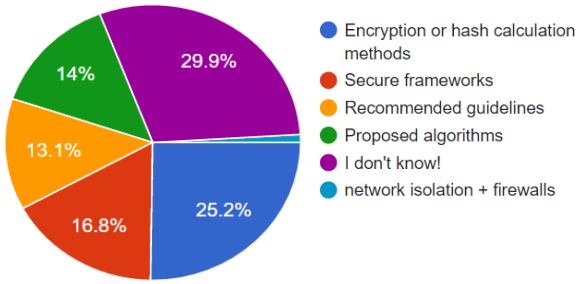

Fig. 7: Cloud threats in surveyed universities.

6. RECOMMENDATIONS

At the end of this study, a few baseline recommendations for cloud administrators within universities for adapting secure cloud computing are presented.

1. The first consideration is to educate the stakeholders adequately on cloud services used in their own network and provide them primary notifications related to security issues. It is recommended to follow security-related guidelines and standards for achieving secure environments such as NIST guidelines for security and privacy.

2. The institution's network must be prepared for cloud computing. This means the network equipment such as routers and firewalls should be configured with critical rules to make cloud network more secure and reach the expected performance. Additionally, setup up network isolation techniques like VPN, VLAN, etc.

3. Make sure that IT administrator able to control and

manage cloud's items and services when concluding the contract agreement with the service provider.

4. An agreement with a third party to perform audits on a regular basis to monitor the performance and compliance of the service provider to the agreed terms.
5. Monitor periodically the performance of available cloud services and resources that have been launched and make a change as required. This procedure may reduce security threats and risks.
6. Applying a threat assessment strategy is an urgent requirement. Sometimes stakeholders were not aware of particular threats to cloud infrastructure. This requires finding a way to discover threats and avoid them before their occurrence. These measures should be taken specially to address potential internal threats.
7. Data and applications in the cloud environment must be classified based on their values according to their importance and sensitivity, not all data stored in the cloud are rated as top secure data. Remember that the use of security tools always effect on the system performance and efficiency.
8. Backup and recovery schemes must be provided to prevent data loss.
9. A proper authentication, authorization, and access security tools and mechanisms should be implemented and regularly monitored.
10. Provide suite strong encryption protocols and key management for data at rest, in transit, and on the backup state.

7. ACKNOWLEDGMENTS

The authors would like to acknowledge all experts, faculty members, and students who have participated and helped us to complete this survey.

8. CONCLUSION

Cloud computing represents an opportunity for universities to take advantages of the enormous benefits of cloud services and resources in the educational process. However, the cloud users remain concerned about security issues that represent the major obstacle that may prohibit the adoption of cloud computing on a large scale.

In this paper, the authors have provided an overview of cloud computing benefits for key stakeholders in the higher educational institution.

The limitations of cloud service models were investigated in addition to challenges and risks threaten cloud computing.

This study shows that the stakeholders are not familiar with possible security risks or procedures used to protect data or cloud application. Furthermore, it indicates that the most serious attacks might threaten cloud networks are Denial of Service (DoS) and phishing attacks.

A comprehensive list of recommendations has been provided to avoid security risks efficiently when adopting cloud computing in educational institutions.

In the future research, the security risks and challenges of virtualization technology will be covered in details to provide a secure infrastructure for IaaS service in the Educational cloud. In addition to focusing on improving QoS provided in cloud computing.

9. REFERENCES

[1] Khalil H. A. Al-Shqeerat, Mohammad Ali A. Hammoudeh, Mohammad Ijaz Abbasi. (2016). Design and Analysis of an Effective Secure Cloud System at Qassim University. International Journal of Computer Science and Information Security (IJCSIS). 14 (8), August 2016, pp.

[2] R. Velumadhava Raoa, K. Selvamanib. (2015). Data Security Challenges and Its Solutions in Cloud Computing, in *Proc.* International Conference on Intelligent Computing, Communication & Convergence (ICCC), Bhubaneswar, Odisha, India, 2015, pp. 204-209.

[3] Mell, P and Grance, T. (2011). The NIST Definition of Cloud Computing. NIST, USA. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[4] Kiran Yadav. (2014). Role of Cloud Computing in Education. International Journal of Innovative Research in Computer and Communication Engineering. 2 (2), pp. 3108-3112.

[5] Niall Sclater. (2010). Cloud Computing in Education. Published by the UNESCO Institute for Information Technologies in Education. Available: http://iite.unesco.org/pics/publications/en/files/3214674.pdf.

[6] Atif Ishaq, M.N. Brohi. (2015). Literature Review of Cloud Computing in Education Sector: A survey with respect to Qatar. International Journal of Computer Applications. 132 (17), pp. 9-14.

[7] Poonam R.Maskare, Sarika R. Sulke. (2014). Review Paper on E-learning Using Cloud Computing. International Journal of Computer Science and Mobile Computing. 3 (5), pp. 1281-1287.

[8] Algirdas A, Jean-Claude L, Brian R, Carl L. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing. 1(1), pp. 11-33.

[9] A.M.Mansuri, Manish Verma, Pradeep Laxkar. (2014). Benefit of Cloud Computing for Educational Institutions and Online Marketing. Information Security and Computer Fraud. 2(1), pp. 5-9.

[10] Amjad Mehmood, Muhammad Roman, M. Munir Umar, Houbing Song. (2015). Cloud Computing Security: A Survey. International Journal of Computer Science and Information Security. 13(7), pp. 20-28.

[11] Dimitrios Zissis, Dimitrios Lekkas. (2010). Addressing cloud computing security issues. Future Generation Computer Systems. 28 (2012) pp. 583–592.

[12] Harshit Srivastava, Sathish Alampalayam Kumar. (2015). Control Framework for Secure Cloud Computing. Journal of Information Security. 6, pp. 12-23.

[13] Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh. (2012). A Novel Open Security Framework for Cloud Computing. International Journal of Cloud Computing and Services Science. 1(2), pp. 45-52.

[14] Yaser Ghanam, Jennifer Ferreira, Frank Maurer. (2012). Emerging Issues & Challenges in Cloud Computing - A

Hybrid Approach. Journal of Software Engineering and Applications. 5, pp. 923-937.

[15] Abdulrahman Alharthi, Fara Yahya, Robert J Walters and Gary B Wills. (2015). An Overview of Cloud Services Adoption Challenges in Higher Education Institutions. In *proc*. Emerging Software as a Service and Analytics, (ESaaSA 2015), Lisbon, 2015, pp. 102-109.

[16] D. Sudha Devi, L.Yamuna Devi, K.Thilagavathy, P.Aruna, N.Priya, S. Vasantha. (2013). Private Cloud in Educational Institutions: An Implementation using UEC. International Journal of Computer Applications. 78(1), pp. 8-12.

[17] Karl van der Schyff, Kirstin E.M. Krauss. (2014). Higher education cloud computing in South Africa: Towards understanding trust and adoption issues. South African Computer Journal. 55, pp. 40-55.

[18] E. Krelja Kurelović, S. Rako, J. Tomljanović. Cloud Computing in Education and Student's Needs. In *proc.* 36th International Convention on Information & Communication Technology Electronics & Microelectronics (MIPRO), Opatija, Croatia, 2013, pp. 726-731.

[19] AlAlaa N. Tashkandi, Ibrahim M. Al-Jabri. (2015). Cloud computing adoption by higher education institutions in Saudi Arabia: an exploratory study. Cluster Computing.18(4), pp 1527–1537.

[20] Hongyu Pei Breivold and Ivica Crnkovic. Cloud Computing Education Strategies. In *Proc.* IEEE 27th Conference on Software Engineering Education and Training (CSEE&T), 2014, pp. 29-38.

[21] Ying Xie, Ken Hoganson. Computing Education on Cloud. In *Proc.* The 2013 World Congress in Computer Science, Computer Engineering, and Applied Computing. Las Vegas, 2013, pp. 479-482.

[22] Mahmoud Odeh, Kevin Warwick, Alexeis Garcia-Perez. (2015). The Impacts of Cloud Computing Adoption at Higher Education Institutions: A SWOT Analysis. International Journal of Computer Applications. 127(4), pp. 15-21.

[23] Vaishali H Pardeshi. Cloud Computing for Higher Education Institutes: Architecture, Strategy and Recommendations for Effective Adaptation. In *Proc.* Symbiosis Institute of Management Studies Annual Research Conference (SIMSARC13). India 2013, pp. 589-599.

[24] S. Subashini, V.Kavitha. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications. 34, pp. 1-11.

[25] Rajarshi Roy Chowdhury. (2014). Security in Cloud Computing. International Journal of Computer Applications. 96(15), pp. 24-30.

[26] Chetan M Bulla1, Satish S Bhojannavar, Vishal M Danawade. (2013). Cloud Computing: Research Activities and Challenges. International Journal of Emerging Trends & Technology in Computer Science. 2(5), pp. 206-214.

[27] Wesam Dawoud, Ibrahim Takouna, Christoph Meinel. Infrastructure as a Service Security: Challenges and Solutions. In *Proc.* The 7th International Conference on Informatics and Systems (INFOS), 2010, pp. 1-8.

[28] Issa M. Khalil, Abdallah Khreishah, Muhammad Azeem. (2014). Cloud Computing Security: A Survey. Computers. 3, pp. 1-35.

[29] Mariana Carroll, Alta van der Merwe, Paula Kotzé. Secure Cloud Computing Benefits, Risks and Controls. In *Proc.* Information Security for South Africa. 2011, pp. 1-9.

[30] Sarang V. Hatwar, R. K. Chavan. (2015). Cloud Computing Security Aspects, Vulnerabilities and Countermeasures. International Journal of Computer Applications. 119(17), pp. 46-53.

[31] Xiangyang Luo, Lin Yang, Linru Ma, Shanming Chu, Hao Dai. Virtualization Security Risks and Solutions of Cloud Computing via Divide-Conquer Strategy. In *Proc.* Third International Conference on Multimedia Information Networking and Security. 2011, pp. 637-641.

[32] Lee Garber. (2012). The Challenges of Securing the Virtualized Environment. Computer. 45(1), pp. 17-20.

[33] Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills. Data Security in Cloud Computing. In *Proc.* Fifth International Conference on Future Generation Communication Technologies (FGCT). 2016, pp. 55-59.