Security Issues Model on Cloud Computing: A Case of Malaysia

Komeil Raisian
Faculty of Information Science and Technology, the National University of Malaysia 43600 UKM Bangi Selangor, Malaysia

Jamaiah Yahaya
Faculty of Information Science and Technology, the National University of Malaysia 43600 UKM Bangi Selangor, Malaysia

***Abstract*—By developing the cloud computing, viewpoint of many people regarding the infrastructure architectures, software distribution and improvement model changed significantly. Cloud computing associates with the pioneering deployment architecture, which could be done through grid calculating, effectiveness calculating and autonomic calculating. The fast transition towards that, has increased the worries regarding a critical issue for the effective transition of cloud computing. From the security viewpoint, several issues and problems were discussed regarding the cloud transfer. The goal of this study is to represent a general security viewpoint of cloud computing through signifying the security problems that must be focused and accomplished appropriately for identifying a better perspective about current world of cloud computing. This research also is to clarify the particular interrelationships existing between cloud computing security and other associated variables such as data security, virtual machine security, application security and privacy. In addition, a model of cloud computing security which depends on the investigation regarding previous studies has been developed. To examine the model a type of descriptive survey is applied. The survey sample population is selected from employers and managers IT companies in Malaysia. By testing the correlation, the results of study indicated that there are those identified security challenges in current world of cloud computing. Furthermore, the results showed that the cloud computing security correlation with data security, virtual machine security, application security and privacy is positive.**

Keywords*—*Cloud Computing; Security Issues; Security Viewpoint; Grid Computing

I. Introduction

Cloud computing refers to the next-generation architecture of IT enterprise. This approach usually focuses on financial utility model by developing several existing methods and computing technology that include distributed application, facilities, and IT infrastructures of computers, networks, and storing capitals [1]. Currently, associated administrations, particularly in small and medium business (SMB) enterprise, assume cloud computing to improve the efficacy and success of their organization as well as decreasing the cost of buying and preserving the organization [2]. Because of the high interest about toward the cloud computing, there is an important worry about the evaluation of the current tendencies in security of that technology. Internet considered as a driving force of the improved technologies and possibly, one of the most important topics in this regard is Cloud Computing. Cloud computing considered as a tendency of the current day scenario, with nearly all the administrations that tried to make it as an entry. Followings are considered as the benefits of using cloud computing: i) decreasing the price of hardware and related maintenance charges, ii) it is easily accessible all over the world, and iii) it has flexible and the extremely automatic procedure, in that the clients are not usually worried about upgrading the software which is a daily manner [3]. Security control events in cloud are identical to old IT settings. Regarding the multi-tenant features, service delivery and deploy models of cloud computing usually associates with the previous IT settings, though, cloud computing might have several risks and problems too [2].The most important goal of this study is to classify, categorize and establish the most important security problems associated with cloud computing which that were discussed in the related literature.

II. Cloud Computing Types and Services Model

To provide a better secure cloud computing clarification, a significant decision relates to the kind of cloud to be applied. Currently three usual utilization approaches of cloud were presented [4]. Initially, private cloud which refers to the private cloud infrastructure set up inside an internal enterprise information center. Regarding this type, it should be noted that, this type is easier to be aligned with security, agreement, and controlling and it can offer a better control over arrangement and practice [5]. Secondly, Public cloud which refers to the cloud infrastructure is usually applied for general public or a big manufacturing groups. Public cloud considered less secure comparing to other related cloud models [6]. And third one refers to the Hybrid cloud which is an alignment of private cloud associated to one or more public cloud services that were restricted through a secure network. Hybrid delivers more secure controlling of the over data [7].

III. Cloud Computing Types and Service Model of Delivery

The second security issue that follows the cloud organization models and should be unpacked by the enterprise management refers to the cloud examination delivery models [8]. The architecture regarding the service delivery models of cloud computing might be characterized in three categories. Firstly, Infrastructure as a Service (IaaS) which considered as the essential computing capitals e.g. storing, network, servers were applied for providing facilities to the final clients. Secondly, Software as a Service (SaaS) which deliver a remote access using a web for operating virtualized and pay-per-use software over the cloud structure .Thirdly, Platform as a

service (PaaS) that refers to the use of equipment and capitals which were delivered by the cloud structure for supporting the end client needs.

IV. Cloud Computing Security Issues

The advantageous of cloud computing that were presented in the related literature covers both fast and easy arrangement, the pay-per-use ideal, and reducing the in-house IT charge. Nevertheless, they also believed that the security considered as the most important subject which should be discussed in the related literature to improve the security of cloud computing application [9]. Main security subjects about cloud computing are as follows:

A. Data Security

Liu [10] believed that cloud computing refers to the quick developments of the users for essay access to the required hardware, software and facilities and other associated capitals in several times. Furthermore, the data security seems to be more important while it is applied for the cloud computing in the SPI background. Cloud computing also faced with several problems, if the experts will not resolve them well, its fast improvement could be affected too. Data security is common in several applications and among the associated problems, it can create many problems for the operators while they keep sensitive data in different cloud servers. These problems refers to the cloud servers which are typically functioned by commercial providers that are very probable to be used outside of the reliable territory of the operators [11].

1) Availability

Certifying timely and consistent contact for using the related data. An obtainability problem refers to the interruption of contact for using the related data or for the data system [12]. Bowers et al. [13] presented HAIL (High-Availability and Integrity Layer), a distributed cryptographic scheme which permits servers to prove to the client that a stored file is complete and retrievable. HAIL strengthens, officially unifies, and streamlines are considered as distinct methods about the cryptographic and distributed-systems groups. Proofs in HAIL are well quantifiable by servers and extremely compact typically tens or hundreds of bytes, regardless of considering the size of the file. HAIL cryptographically confirms and reactively changes file shares. It is strong against a dynamic, mobile opposition, i.e., one which might increasingly corrupt the full different servers. Bowers et al. [13] suggest a perfect, official adversarial approach for HAIL, and difficult examination of element choices, in which the researcher showed how HAIL progresses the safety and efficacy of current equipment, such as Proofs of Retrievability (PORs) that is organized on separate servers.

2) Confidentiality

Preserving authorized limitations about the data accessibility and release, like the tools for keeping the individual privacy and exclusive data, a loss of privacy is the illegal disclosure of data [12]. About some useful application arrangements, the privacy of the information is not considered merely a security/privacy subject, but a juristic problem. As an example, in healthcare application projects using the Protected Health Information (PHI) must follow the necessities of Health Insurance Portability and Accountability Act (HIPAA), and making the user information private in the storage servers is not just considered as a possibility. Data confidentiality might likewise attained while Cloud Servers cannot learn the plaintext of related data file in the system [11].

3) Integrity

Guarding against unsuitable data adjustment or destruction and safeguarding the data, non-repudiation and truthfulness, a loss of truthfulness is the unauthorized change or destruction of data [12]. One big problem about the cloud data storage refers to the data integrity confirmation at untrusted servers. As an example, the storage service supplier, that experiences Byzantine problem infrequently, might decide to hide the information errors of the users for their own benefits. The more serious issue is that by saving money and the storage space, the service provider may ignore keeping or deliberately delete the infrequently retrieved information files that belongs to a normal user. By considering the large dimension of the outsourced electronic information and the customer's forced resource competence, the core of the problem might be widespread as how can the customer find an effective method for performing periodical integrity confirmations without copying the local information files [14].

4) Data location

Several regulations for managing the information might vary from country to country. Consequently, transporting confidential information among the countries could be considered as a challenging task. Regarding the cloud setting, the position of the information centers and backups should be understood perfectly to ensure that legal problems wouldn't happen [15]. By using the Cloud Computing, users will have the chance of using data mobility capabilities to a high extent and customers do not typically know the location of their information and in many cases, it is not considered as big challenge for the users. As an example, emails and photographs that were uploaded to the Facebook might exist all over the world and Facebook users are commonly not concerned about this matter. Nevertheless, once an enterprise has some sensitive information which is kept on a storage device of the Cloud, they might want to see its location too. Moreover, they might also want to identify a favored location (e.g. information to be reserved in the UK), then they needs a contractual contract among the Cloud service providers and customers, in that information must stay in a specific position or exist in on a specified recognized server [16].

5) Data Recovery

Data Recovery considered as an important section of each Business Continuity Planning. By applying an unrestricted cloud provider, it should be noted that the Business Continuity Planning and the Data recovery could be expanded to contain catastrophes which affects the public cloud provider. About natural problems or related disasters, a cloud service provider information center might be inaccessible. About this possibility, it is important to apply a well-thought out disaster retrieval strategy [17]. An event like a server breakdown might cause injury or loss about the users' information. To avoid this issue, users should do a backup from the data for the recovering in the future. Additionally, cloud users can save backup of important data on a local computer [1].

6) Retention

How long could the personal data which was transported to the cloud retained? Who applies the preservation strategy about the cloud, and how we can manage litigation holds [18]. How long we can retain the personal information which were transferred by the cloud? Who imposes related retention policies in the cloud environment, and how we can manage our exceptions regarding this policy (like the litigation holds). Logs typically contain timestamps and timing information considered important for the compliance of laws and policies about the data retention, so it seems important to have a data retention and destruction strategy for all related data storing schemes. Timing activates might also decrease the data which should be recorded as the temporary information which is merely kept for doing current transaction and formerly deleted that has minimal confidentiality implications [19].

7) Ownership

Typically, workers or administrations have accessibility to the information and they can manage them well. Once the information moved to the cloud, we have to consider how we can maintain the Information possession [20]. Data ownership refers to the clouded initial move of the cloud, with queries about what happens to information while it moves to the cloud? What occurs while a cloud provider goes out of industry? In addition, what occurs if cloud clients could not pay their bills? [20]. Cloud computing did investigations about the virtualization, distributed computing, utility computing, and during the recent years on networking, web and software facilities. It suggests a service-oriented architecture, limited data technology overhead for the end-client, having high flexibility, decreased total cost of possession, on request facilities and many related matters.

8) Access control

Regarding the cloud setting, the association between capitals and operators considered very commercial hoc and active resource workers and customers are not usually located in a similar security field while clients are typically recognized by their features or qualities, not predefined characteristics. Consequently, the old-style character based access control models are not effectual, and access decisions should be made according to the qualities. Diplomas delivered by a PKI facility might be applied to enforce admission control in the Web setting [21]. Access Control permits one application to trust the individuality of related application. The old model for accessing control is application-centric access control, where per application keeps related tracks of its user collection and manages them which is not practical in cloud founded architectures, as in this approach we need lots of memories to store the details of the users like their username and password. Consequently, cloud needs a user centric access control while every operator request to the related service provider that is bundled with the user character and right data [22].

9) Data lock-in

In the other word, the clients cannot move easily from a SaaS or IaaS vendor to the other one. The client data could be destroyed, that stop users to adopt cloud Computing. Coghead recognized as an example of a cloud platform whose shutdown left clients scrambling, to reword their requests for running on the other platform and the solution is to regulate cloud Application Programming Interface (API) [1]. Weiss [23] believed that software considered as a service in the cloud that might recover doubts about the vendor information lock-in as an important concern in the processer era. Assuming a cloud worker and a thin-client seller partner together, it is likely that per half will need the other. Services about the cloud might be unreachable to those without an access tool from a single brand. Some believe that the cloud could inspire the development of walled-gardens, a potential step back associated to the comparatively open internet of today.

B. Virtual machine level security

Virtual setting contains different VMs, which deliver self-governing security areas. It is hard to manage several VMs effectively, working on a similar physical organization. The most important purpose of Virtualization refers to the way it certifies several VM examples working on a similar physical engine that are separated from each other [24, 25]. Virtual machines (VMs) considered as the most common form to provide the computational capitals of cloud operators at this layer, where the operators get finer-granularity flexibility as they generally get super-user access to their VMs, and may use it to modify the software stack on their VM for presentation and efficacy and frequently, such facilities are dubbed Infrastructure as a Service (IaaS). Virtualization considered as an enabler technology for this cloud component that permits users of unparalleled flexibility to arrange their locations while protecting the physical organization of the providers' information center. Recent progresses in OS Virtualization made the IaaS concept believable. This was exactly enabled by two virtualization methods namely; par virtualization and hardware-assisted virtualization. Though both virtualization skills concerned with the performance separation among virtual machineries opposing on shared resources, performance interference among VMs shares, and similar cache and TLB hierarchy cannot yet be evaded [26].

1) Hypervisor security

Hypervisor considered as a key software constituent of Virtualization. It usually affects all VMs acts working with the Virtualization host. While an attacker totally controls a hypervisor, then he may apply any activity to the VMs on the host scheme. Two stages in security administration of hypervisor were proposed [1, 24 and 18]. Regarding a real hypervisor product, like Xen, OpenVZ or VMware, the attacker usually attempt to exploit the security holes to modify the hypervisor, so that he may install a rootkit on it. The solution is to update and patch the hypervisor product and other virtualization products regularly. Furthermore, the investigation of how different components in the hypervisor architecture work, like monitoring the actions of the guest VMs and intercommunication amongst different infrastructure machineries, might contribute improving the security of cloud system. Two stages in security administration of hypervisor were proposed that will follow [1, 24 and 18].

2) Authorization and Authentication

Authorization and Authentication are considered as the most significant features of managing a virtual host reviewing goal. Authorization confirms that clients should be authorized

and have consent to do their required tasks. For the authentication, suitable values and existing instruments should be applied to validate related account correctly [27]. Youseff [26] believed that before persuading customers for migrating from desktop to cloud applications, cloud applications' providers should consider different users' concerns regarding both security and safety of keeping private information on the cloud, users' verification and approval, up-time and presentation, backing up the data and problems for recovering and providing reliable SLAs about their cloud applications.

3) Networking

Network communications and arrangements are considered as the important security subjects about the cloud computing organizations. Cloud computing embraces cyber infrastructure, and shapes upon periods of investigation in virtualization, dispersed computing, "grid computing", utility computing, and more lately, networking, web and software amenities. It usually refers to the service oriented architecture, reduced information technology designed for the users, being more flexible, reduced entire charge of ownership, on request facilities and several other issues [20]. It is significant to deliver a mechanism for the assurance of secure assembly of the organization in the safety zone that has three instruments [24]. Firstly, transfer security that it is Cloud computing circulated architectures contain a huge resource sharing and virtual engine instance synchronization. Therefore, it needs VPN machineries to protect the cloud scheme against sniffing, spoofing and side-channel problems. Secondly, firewalling which refers to the protection of the provider's interior cloud substructure, Firewalls can deliver protection from insider and outsider and permit VM isolation, fine-grained filtering about the addresses and ports and preventing the Denial-of-service (DoS). It is significant to improve a reliable firewall and other safeties regarding the cloud contexts. Thirdly, Security configuration that usually focuses on the formation of protocols, schemes and skills for meeting predictable level of security and confidentiality without cooperating performance of efficacy.

4) Isolation

In the virtual setting of cloud computing, although it reasonably isolated, all VMs have the same hardware and therefore the similar capitals. This might clue to exploit of data leaks and cross-VM attack. For better protection the notion of separation might also be used for a better fine-grained properties, like computational capitals, storing and memory [1]. The most important feature of virtualization refers to the ensuring of VM instances running on a similar physical mechanism that are separated from each other. Though, in the isolation technologies current VMMs offer and the control of manager on host and guest working schemes are not considered good that leads to several security matters of virtualization [1]. Virtual machine technology delivers strong isolation among virtual areas. As an example, security isolation avoids a malicious application to attack applications or retrieving information in other areas. Fault isolation avoids one fault application to bring down the entire system. Environment isolation permits several operating schemes for running on a similar machine, accommodating legacy applications and cutting-edge software, each with a distinct set of arrangements and elements [28].

C. application security

Application security refers to the use of system capitals, such as software and hardware for secure requests which holds them in contradiction of malicious saturation that attacks the cloud. Though there is a security program in cloud computing like Quad Core Intel Xeon Processors and IP address [30], but still there are several problems in security at application step which might permit unlawful clients to have access. Consequently, cloud is usually insecure the application due to the security holes like unconfident software Connectors or APIs interrelating with cloud facilities. There are different threats regarding the security program of the cloud [29].

1) Cloud browser security

In Saas module Customers computing tasks are allocated to the remote server. The client system is usually applied for the IO take and sends instructions to the cloud. Though there are several security matters in cloud, but browser security is very significant, particularly in cloud computing [31]. Browser might only be applied in the encryption and signature Transport Layer Security (TLS) that usually have enough security to define the malicious attacks. Solution provided Simultaneous application of TLS and XML is founded encryption at the central of the browser [32]. Web browsers might not openly apply XML Signature or XML Encryption and information might merely be encoded over TLS, and signatures are merely applied inside the TLS handshake. For all other cryptographic information circles inside WS-Security, the browser merely serves as the passive information store. Several simple workarounds were planned to be used e.g. TLS encryption instead of XML Encryption, but the main security challenges with this method were elaborated in the literature and working attacks were applied as proofs-of concept (cf. 3.2.2). Our purpose is to suggest provably secure solutions applying TLS, but at the same time inspire the browser community to adopt XML founded cryptography to be included in the browser core [32].

2) Cloud malware attack

This kind of attack injects VM malicious or implementation service to cloud computing organization and its goal it is to vary extensively, either stopping, eavesdropping or adapting information by adapting the delicate about overall Capability variations. The aggressive make VM destructive instance of model Implementation Services like, Saas, Iaas and add it to cloud computing. And its answer refers to the implementation of integrated review, like Services before using it for received desires along the cloud scheme [33]. Bhadauria et al. [29] believed that apart from the above stated network, related problems are regarded to dissimilar security problems in a mobile cloud computing setting. By using the applications lying over the cloud, it is likely for the hackers to corrupt an application and gain access to the mobile device once opening that application. To avoid those conditions, strong virus scanning and malware security software should be installed to prevent any kind of virus/malware check into the mobile scheme. Likewise, by inserting device identity guard, like permitting access to the authorized operator according to some

form to identity check feature that will let blocking unauthorized admission.

3) Backdoor and debug option

The majority of the designers write code which are backdoor requested or unwanted. They might likewise stop some debugging choices for testing or revising the website again. In Saas and Paas models, though backdoors are in these contexts, but some hackers can simply enter website and use the important related data. These concepts must be resolved at the advanced level [34]. A usual habit of the designers is to permit the debug choice when publishing a web-site. This allows them to make developing variations in the code and getting them executed in the web-site. Since these debug options are considered ease backend admission to the inventers, and occasionally these debug choices are left allowed unnoticed, it might deliver an easy possibility for the hacker to enter the web-site and allows him/her for making variations at the web-site level [29].

4) Cookie poisoning

It points to the illegal contact or web requests by Identify bases of cookie. In Saas model, Cookies defense of data permits requests for detecting illegal user identification and these cookies are obtainable. They might be invented for shaping the individuality of an illegal user [29]. The threats to application level security contain XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, DoS attacks, Backdoor and Debug Options, CAPTCHA Breaking etc subsequent from the illegal usage of the applications. It includes altering or adapting the contents of cookie for making unauthorized accessibility to an application or to a webpage. Cookies essentially include the identity of the user related credentials and when these cookies are available, the content of those cookies could be forged to imitate an authorized operator. This might be evaded either by doing regular cookie cleanup or applying an encryption system about the cookie information [29].

5) Privacy

The data of operators are usually sored in the data center, then the cloud provider allocate them among hundreds of servers that wish to have risk possibility. These facilities are applying internet as announcement, presenting online software, so cloud providers particularly [Iaas] would be involved with risks [35]. Once the users attempt to use their hidden data from cloud provider examination in this period, they would lose the information. This is considered, as good chance for attackers, they would examine to submit data by operators [34]. Some data refers to the name, address, religion, race, well-being job performance, credit card number which depends on the type of cloud provider facilities [36]. Cloud providers particularly [Iaas] offer to their users that the data storage frequently bring a frictionless of the procedure of registration, as it lets someone to use cloud service and there are several indications that hackers instigated to target [Iaas] retailers [37]. Based on the cloud-based amenities customer's information kept in third-party part [38]. Consequently, service provider should measure the amount of information security precisely for ensuring the privacy of the information. One way for enhancing the safety is incorporation of information encryption. In the other words, incorporation information encryption with data could be done to protect the information of the user against hackers, and it will be helpful to limit the accountability of service providers. Wen and Xiang [39] believed that the protections against malicious hackers who might have access to the service provider's scheme considered as the final goal which is not sufficient. We might face several dangers once providers attempt to recover the related information. Consequently, how providers may improve the customer's information? It seems to be easy that user only find the cloud provider that he/she can trust. This method considered appropriate once the data is not so significant. This approach is suitable to recover the data in small company for finding the reliable provider. Surly, it might be a problem in that company, but for medium-sized to maximum-sized firm, it is logical to find a solution than finding reliable provider for information retrieval. They must expand techniques and approaches over the information encryption to ensure the privacy of cloud provider or apply private cloud could be a better clarification in these businesses.

V. PROPOSED MODEL

The quantitative study method had been useful for this research. Figure 1 shows the proposed model of this research to know the effects of the factors (data security, virtual machine security, application security and privacy) on cloud computing security in current world of cloud computing based on enlists main studies indicating main factors in Table 1. This model presents the relationships between Main Security factors on Cloud Computing and indicates how those components are positively associated with it. The final results involving SPSS tested the correlation of those factors with cloud computing security based on sample population is selected equal with 150 that is randomly obtained from employers and managers IT companies in Malaysia. Figure 1 exhibits the particular associations concerning these factors and Cloud Computing security as well. Questionnaires were arranged to be determined by these factors. This section supplied the reason on the four factors independently and together with their investigation from the questions gotten by respondents of the research. This reason was taken by the researcher to come up with a model as it is presented in Figure 1. The model combines those factors that had not really been connected from the previous researcher. The researcher examined impacts of each component in suggested model through conducting an additional study in the various firms from the previous one.

TABLE I. CLUSTERING SORTS OF CLOUD COMPUTING SECURITY

Articles	Cloud computing security			
	Data security	Virtual Machine Security	Application Security	Privacy
[10]	*			
[13]	*			
[12]	*			
[11]	*	*		
[14]	*			
[16]	*			
[17]	*			
[18]	*	*		
[19]	*			
[20]	*	*		
[21]	*			
[22]	*			
[23]	*			
[24]		*		
[25]		*		
[30]			*	
[27]		*		
[26]		*		
[28]		*		
[29]			*	
[32]			*	
[33]			*	
[34]			*	
[36]				*
[35]				*
[37]				*
[38]				*
[39]				*
[15]	*	*		
[30]			*	
[31]			*	
Total	14	9	8	5

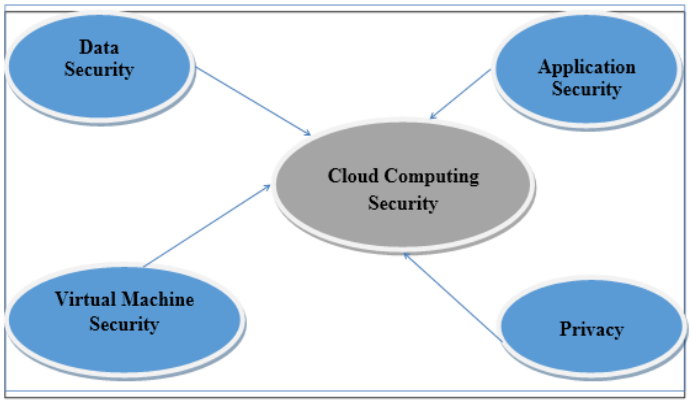

Fig. 1. Research Proposed Model

VI. THE RELATIONSHIP OF SECURITY CLOUD COMPUTING FACTORS

This study had recently mentioned data security, virtual machine security, application security and privacy as main factors of proposed cloud computing security model. Therefore, this section aims to examine the correlation of these seven factors with cloud computing security. Common produced variances are all above the advised 0.5 degrees, Anderson and. [40] stated that supporting the discriminate validity of measurement scales supporting the discriminate validity of measurement scales. Correlation indicates the strong of a linear relationship between two variables. The created correlation coefficients that symbolize the strength of these relationships relating to the research variables are shown in Table 2.

It is obvious from Table 2 that the correlation coefficients on the connections between research variables can be found strong. In addition, within Table 2, the correlation coefficient value is 0.706 between Data Security (DS) and Cloud Computing Security (CUS) variables that indicates these variables are strongly correlated since it is greater than 0.5. Virtual Machine Security (VMS) is found to be strongly related to CUS and the correlation coefficient value is 0.722. Application Security (AS) is found to be strongly related to CUS with correlation coefficient equal with 0.699. Furthermore, Privacy (Pri) is strongly related to CUS with the correlation coefficient value of 0.675. The results still support our proposed model. While our results show that whole, factors on current world of cloud computing are indeed distinct constructs and it also appears that all factors are well correlated with Cloud Computing Security.

VII. CONCLUSION

Cloud computing ensures having an extensive effect on the schemes and networks of organization and other initiatives and it focuses on cost decrease, high performance and benefit of cloud computing in the administrations .One of the gorgeous trait in cloud computing might refer to the difference between classic security plan and control. Classifying the safety of complicated computer system that joint together is a long time security subjects regarding the computing in overall cloud computing. Access to high qualities considered as the main purpose in applying the cloud computing security experts and workers. Public cloud computing considered as a critical factor that enterprises needs for combining their Information as a solution package. The enterprises must be ensured that related activities about security and confidentiality is happening correctly in their business. Assessing management risk in cloud computing systems could be changed in several organizations.

TABLE II. INTER-ITEM CORRELATION

Correlations					
	DS	VMS	AS	Pri	CUS
DS	1	0.690	0.810	0.750	**0.706****
VMS	0.690	1	0.720	0.845	**0.722****
AS	0.786	0.825	1	0.789	**0.699****
Pri	0.780	0.845	0.794	1	**0.675****
CUS	0.620	0.755	0.825	0.794	1
** Correlation is significant at the 0.01 level (2-tailed).					
a. Listwise N = 150					

Likewise the system must have a balance against obtainability of privacy and security's control. Administrations must evaluate the fit balance among the number and strength of the control and hazards associated with the cloud computing solutions. This research also clarifies this purpose and its relationship with cloud computing security within four crucial constructs in cloud computing. By testing the correlation, the results of study indicated that the results of study indicated that there are those identified security challenges in current world of cloud computing. In addition, the results showed that the cloud computing security correlation with data security, virtual machine security, application security and privacy is positive. Between cloud computing security and other associated variables such as data security, virtual machine security, application security and privacy.

ACKNOWLEDGMENT

First and foremost praise be to Almighty Allah for all his blessings for giving me patience and good health throughout the duration of this research. I wish to thank my supervisor and my family for their love, support, encouragement and sacrifice throughout the course of this study. Last, but not least, I would like to thank my beloved wife for standing by me no matter how rough the sea and the journey has been. She is the only one that can attest to all sacrifices we both had to make, so that this manuscript can become a reality.

REFERENCES

[1] You, P., Peng, Y., Liu, W., & Xue, S. (2012, June). Security issues and solutions in cloud computing. In Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on (pp. 573-577). IEEE.

[2] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647-651). IEEE.

[3] Maggiani, R. (2009, July). Cloud computing is changing how we communicate. In Professional communication conference, 2009. IPCC 2009. IEEE international (pp. 1-4). IEEE.

[4] Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In Information Security for South Africa (ISSA), 2010 (pp. 1-7). IEEE.

[5] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), 7-18.

[6] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[7] Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing. John Wiley & Sons.

[8] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[9] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.

[10] Liu, X. (2014, January). Data Security in Cloud Computing. In Proceedings of the 2012 International Conference on Cybernetics and Informatics (pp. 801-806). Springer New York.

[11] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). Ieee.

[12] Winkler, V. (2011a). Chapter 1 - Introduction to Cloud Computing and Security Securing the Cloud (pp. 1-27). Boston: Syngress.

[13] Bowers, K. D., Juels, A., & Oprea, A. (2009, November). HAIL: a high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 187-198). ACM.

[14] Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, March). Privacy-preserving public auditing for data storage security in cloud computing. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). Ieee.

[15] Kumar, P., & Arri, H. S. (2013). Data Location in Cloud Computing. International Journal for Science and Emerging Technologies with Latest Trends, 5(1), 24-27.

[16] Mahmood, Z. (2011, September). Data location and security issues in cloud computing. In Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on (pp. 49-54). IEEE.

[17] Sitaram, D., & Manjunath, G. (2012). Chapter 7 - Designing Cloud Security Moving To The Cloud (pp. 307-328). Boston: Syngress.

[18] Popovic, K., & Hocenski, Z. (2010, May). Cloud computing security issues and challenges. In MIPRO, 2010 proceedings of the 33rd international convention (pp. 344-349). IEEE.

[19] Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011, July). TrustCloud: A framework for accountability and trust in cloud computing. In Services (SERVICES), 2011 IEEE World Congress on (pp. 584-588). IEEE.

[20] A Vouk, M. (2008). Cloud computing–issues, research and implementations. CIT. Journal of Computing and Information Technology, 16(4), 235-246.

[21] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592. pp.163-275.

[22] Onankunju, B. K. Access Control in Cloud Computing. International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013 1 ISSN 2250-3153

[23] Weiss, A. (2007). Computing in the clouds. networker, 11(4).

[24] Dorey, P. G., & Leite, A. (2011). Commentary: Cloud computing–A security problem or solution?. information security technical report, 16(3), 89-96.

[25] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing, 1(1), 1-18.

[26] Youseff, L., Butrico, M., & Da Silva, D. (2008, November). Toward a unified ontology of cloud computing. In Grid Computing Environments Workshop, 2008. GCE'08 (pp. 1-10). IEEE.

[27] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy, 8(6), 24-31.

[28] Koh, Y., Knauerhase, R. C., Brett, P., Bowman, M., Wen, Z., & Pu, C. (2007, April). An Analysis of Performance Interference Effects in Virtual Environments. In ISPASS (pp. 200-209).

[29] Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388.

[30] Intel Corporation, "Delivering Application-Level Security at Data Centre Performance Levels," http://download.intel.com/netcomms/technologies/security/320923.pdf , 2008.

[31] Google, "Browser security handbook," http://code.google.com/p/browsersec /, 2009.

[32] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In Cloud Computing, 2009. CLOUD'09. IEEE International Conference on (pp. 109-116). IEEE.

[33] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

[34] Hacker4Lease, "Backdoor and Debug Options," http://www.hacker4lease.com/attack-methods/backdoor / , 2011.

[35] Almond, C. (2009). A practical guide to cloud computing security. A white paper from Accenture and Microsoft.

[36] Yang, J., & Chen, Z. (2010, December). Cloud computing research and security issues. In Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on (pp. 1-3). IEEE.

[37] Mead, N. R., & Stehney, T. (2005). Security quality requirements engineering (SQUARE) methodology (Vol. 30, No. 4, pp. 1-7). ACM.

[38] Lombardi, F., & Di Pietro, R. (2011). Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34(4), 1113-1122.

[39] Wen, H., Hai-ying, Z., Chuang, L., & Yang, Y. (2011, August). Effective load balancing for cloud-based multimedia system. In Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on (Vol. 1, pp. 165-168). IEEE.

[40] Anderson, E. W., Fornell, C., & Lehmann, D. R. (1994). Customer satisfaction, market share, and profitability: findings from Sweden. The Journal of Marketing, 53-66.