# Cloud Computing and Security Issues in the Cloud

**2 authors**, including:

Monjur Ahmed
Waikato Institute of Technology
**12** PUBLICATIONS   **85** CITATIONS

**Some of the authors of this publication are also working on these related projects:**

Distributed and decentralised software architectures  View project

# CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD

Monjur Ahmed[1] and Mohammad Ashraf Hossain[2]

[1]Senior Lecturer, Daffodil Institute of IT, Dhaka, Bangladesh.
[2]Freelance IT Consultant, Dhaka, Bangladesh.

*ABSTRACT*

*Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure.*

*KEYWORDS*

*Cloud computing, cloud service, cloud security, computer network, distributed computing, security.*

## 1. INTRODUCTION

Recent developments in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012; Singh & jangwal, 2012). Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one. There have been a number of different blends that are being used in cloud computing realm, but the core concept remain same – the infrastructure, or roughly speaking, the resources remain

somewhere else with someone else's ownership and the users 'rent' it for the time they use the infrastructure (Bisong & Rahman, 2011; Rashmi, Sahoo & Mehfuz, 2013; Qaisar & Khawaja, 2012). In some cases, stored sensitive data at remote cloud servers are also to be counted. Security has been at the core of safe computing practices. When it is possible for any unwanted party to 'sneak' on any private computers by means of different ways of 'hacking'; the provision of widening the scope to access someone's personal data by means of cloud computing eventually raises further security concerns. Cloud computing cannot eliminate this widened scope due to its nature and approach. As a result, security has always been an issue with cloud computing practices. Robustness of security and a secured computing infrastructure is not a one-off effort, it is rather ongoing – this makes it essential to analyse and realize the state-of-the-art of the cloud computing security as a mandatory practice. Cloud is mainly categorized as private cloud, community cloud, public cloud and hybrid cloud (Ogigau-Neamtiu, 2012; Singh & jangwal, 2012; Rashmi et al., 2013; Qaisar & Khawaja, 2012; Kuyoro, Ibikunle & Awodele, 2011; Suresh & Prasad, 2012; Youssef, 2012) - the discussion in this paper assumes only one category of cloud exists which is public cloud; as this assumption will well satisfy all the characteristics of any other type of cloud. Due to its diversified potentiality, the approach to cloud computing is being thought to be as the 5th utility to join the league of existing utilities water, electricity, gas and telephony (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009) rather than being just another service.

The study presented in this paper is organized with a view to discuss and indentify the approach to cloud computing as well as the security issues and concerns that must be taken into account in the deployment towards a cloud based computing infrastructure. Discussion on the technological concepts and approaches to cloud computing including the architectural illustration has been taken into consideration within the context of discussion in this paper. Security issues inherent in cloud computing approach have been discussed afterwards. The exploration in the technological and security concerns of cloud computing has led to the concluding realization on the overall aspects of cloud computing. The approaches to counter security issues inherent in cloud computing are numerous with diversified facets and applications which has been kept out of scope. A discussion on the authentication of cloud computing has been addressed as it forms the holistic basis to embed integrity in the context of cloud computing security.

## 2. CLOUD COMPUTING INFRASTRUCTURE

The term cloud computing is rather a concept which is a generalized meaning evolved from distributed and grid computing. Cloud computing is described as the offspring of distributed and grid computing by some authors (Che, Duan, Zhang & Fan, 2011).The straightforward meaning of cloud computing refers to the features and scenarios where total computing could be done by using someone else's network where ownership of hardware and soft resources are of external parties. In general practice, the dispersive nature of the resources that are considered to be the 'cloud' to the users are essentially in the form of distributed computing; though this is not apparent or by its definition of cloud computing, do not essentially have to be apparent to the users.

In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in the cloud. Where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier, the term 'cloud computing' is rather a concept, so are the terminologies to define different blends of cloud computing. At its core essence, cloud computing is nothing but a specialized form of grid

and distributed computing which varies in terms of infrastructure, services, deployment and geographic dispersion (Hashizume et al. 2013; Westphall et al., 2011; Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010). In a pervasive meaning within the context of computer networks, infrastructure could be thought of as the hardware as well as their alignment where platform is the operating system which acts as the platform for the software (Singh & jangwal, 2012; Lee, 2012). Thus the concept of cloud based services is hierarchically built from bottom to top in the order of IaaS, PaaS and SaaS. This is merely the level of abstraction that defines the extent to which an end-user could 'borrow' the resources ranging from infrastructure to software – the core concern of security and the fashion of computing are not affected by this level of abstraction. As a result, security is to be considered within any form of cloud computing (Bisong & Rahman, 2011) regardless of flavour, hierarchy and level of abstraction. Virtualization is an inevitable technology that is highly coupled with the concept of cloud computing (Buyya et al.,  2009; Ogigau-Neamtiu, 2012; Hashizume et al. 2013; Kim, 2009; Mosher, 2011; Atayero & Feyisetan, 2011; Zissis & Lekkas, 2012) – it is the virtualization technology that complements cloud services specially in the form of PaaS and SaaS where one physical infrastructure contains services or platforms to deliver a number of cloud users simultaneously. This leads to the addition of total security aspects of virtualization technology on top of the existing security concerns and issues of cloud computing.

Figure 1 illustrates a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture.
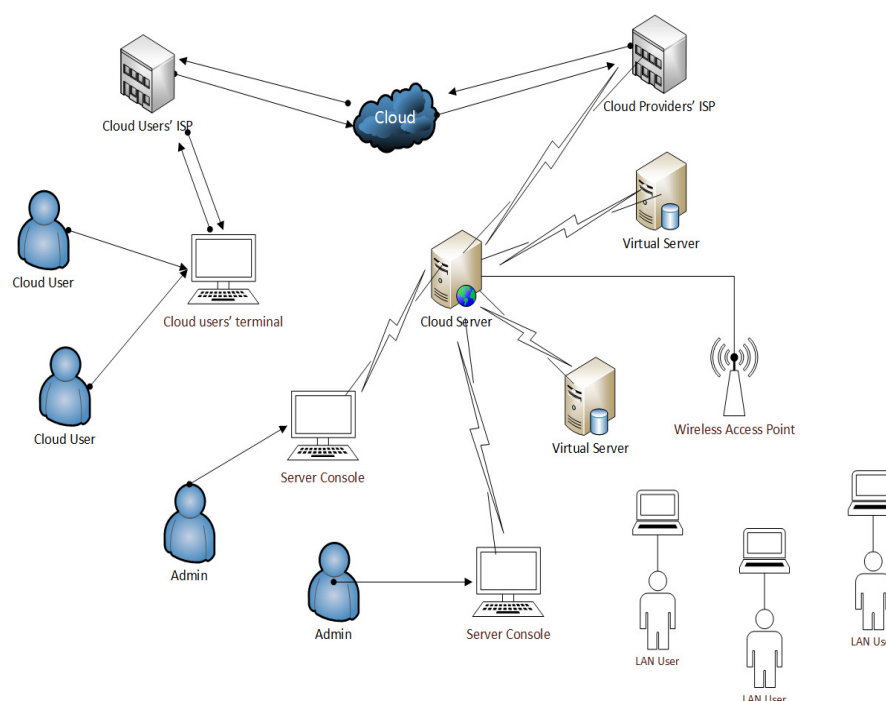


Figure 1: A Typical Cloud Architecture

The illustration of cloud architecture in figure 1 is a simplest one where few complex characteristics of cloud computing (e.g. redundancy, server replication, and geographic dispersion of the cloud providers' network) are not shown – the purpose of the illustration is to establish the arrangement that makes the concept of cloud computing a tangible one. The network architecture

is self explanatory with the identification of cloud users when considered in-line with the discussion of the cloud computing concept presented earlier. One notable part from the architecture is that, while the cloud users are clearly identified and named accordingly due to their remote location and means of remote access to the cloud servers, the admin users who are administering the cloud servers are not cloud users in any form with respect to the cloud service provider's network in the scenario. It is arguable whether the LAN users in figure 1 are cloud users or not. Such room for argument could exist due to the phrase 'cloud computing' being a concept rather than a technical terminology. If the definition of cloud computing is taken to have essential arrangements of being the servers located remotely that are accessed through public infrastructure (or through cloud), then the LAN users in figure 1 may not be considered as the cloud users in the context. With respect to distributed and grid computing as the mother technology that define the infrastructural approach to achieve cloud computing, the LAN users in the scenario are essentially the cloud users when they use the cloud services offered by the servers; the LAN users in this perspective are essentially using resources that are 'borrowed' from the servers on an on-demand basis.

Figure 2 illustrates the hierarchical arrangement based on which a cloud is perceived in the form of IaaS, PaaS and SaaS from any cloud end-user's viewpoint.
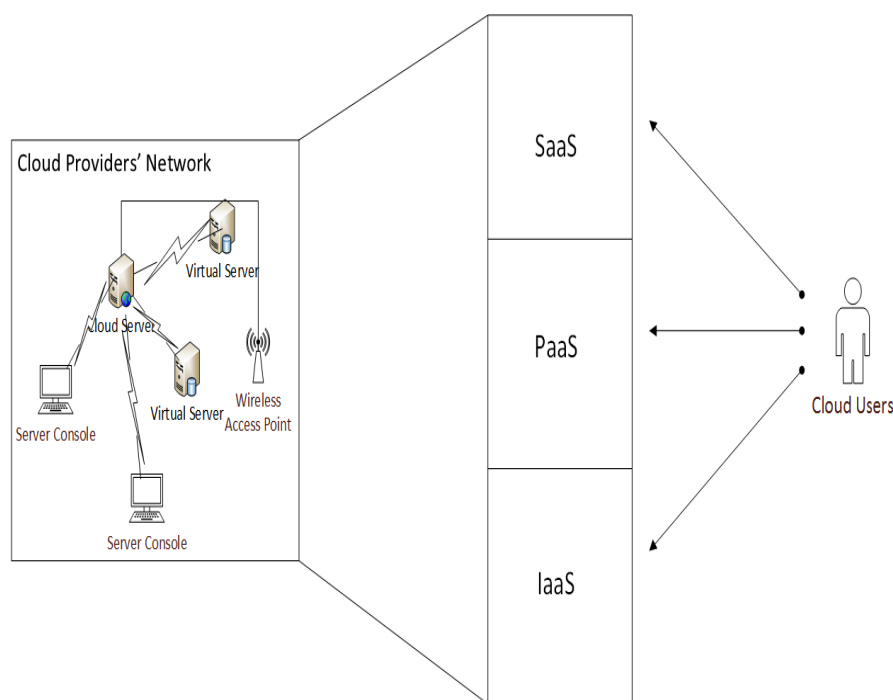


Figure 2: Cloud Service Hierarchy

As depicted in figure 2, the technical details, arrangements and management of the cloud service providers' network is transparent to the cloud user. From the end of the cloud user, the service from the provider comes in the form of SaaS, PaaS or IaaS where the cloud user has no intention or worry about what goes on in the internal arrangement of the cloud service providers' network. Any disruption of any form for whatever is the reason, deem to the cloud users either as service unavailability or quality deterioration – its affect and ways to counter this disruption is a critical part for the cloud infrastructure. Security issues might play a stimulating role as a driving factor for any aforementioned disruption.

## 3. AUTHENTICATION IN CLOUD

Security is the most prioritized aspect for any form of computing, making it an obvious expectation that security issues are crucial for cloud environment as well. As the cloud computing approach could be associated with having users' sensitive data stored both at clients' end as well as in cloud servers, identity management and authentication are very crucial in cloud computing (Kim & Hong, 2012; Emam, 2013; Han, Susilo & Mu, 2013; Yassin, Jin, Ibrahim, Qiang & Zou, 2012). Verification of eligible users' credentials and protecting such credentials are part of main security issues in the cloud - violation in these areas could lead to undetected security breach (Kumar, 2012) at least to some extent for some period. A possible authentication scenario for a cloud infrastructure is illustrated in figure 3.
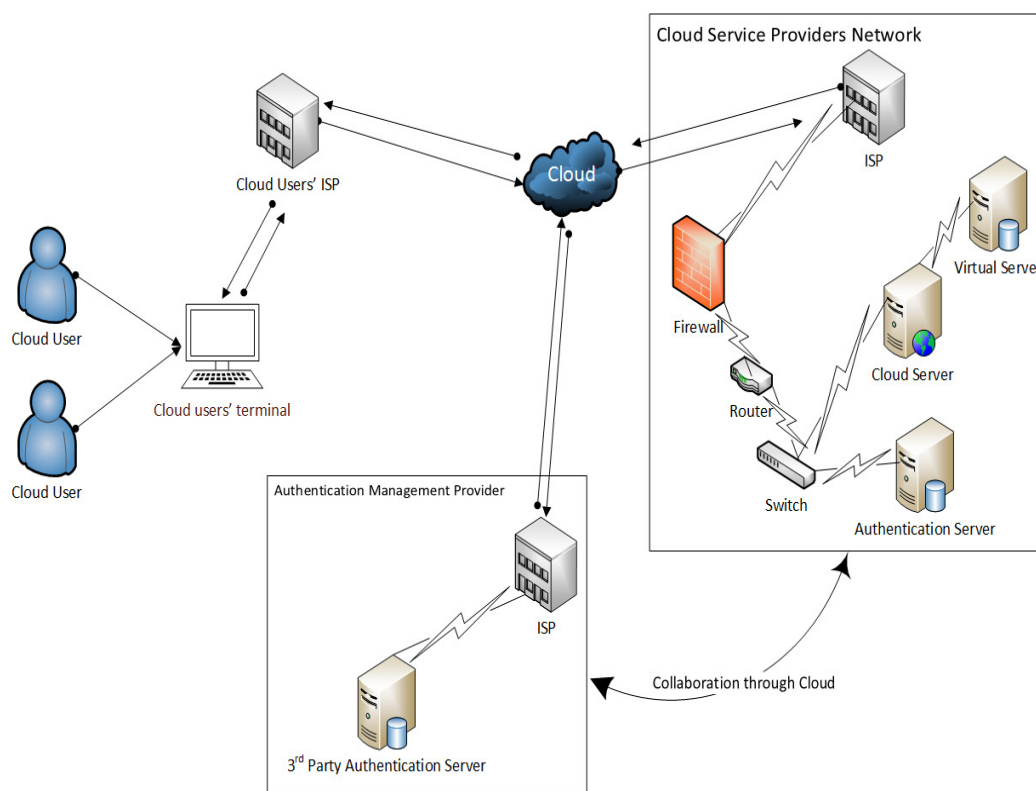


Figure 3: Authentication in the Cloud

The illustration presented in figure 3 conveys that the authentication for the cloud users can be done either by the cloud service provider or the service provider can outsource the identity management and authentication service to third party specialists (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Naslund & Pourzandi, 2012; Sharma & Mittal, 2013). In the later case, the cloud service provider is required to have collaboration with the third party authentication specialist – the collaboration between the cloud service provider and the third party authentication specialist during the authentication process of cloud users is done essentially through cloud. This feature adds performance overheads and security issues to the cloud context as the message passing between third party authentication management authority and the cloud service provider as part of collaboration might essentially be done through cloud infrastructure. As discussed earlier, the total authentication process and how they are carried out - regardless of the involvement of third party authentication specialists – is transparent to the cloud users. The

illustration on the authentication scenario presented above is a fairly simple one – if geographically dispersed servers are deployed by the cloud service providers then the total authentication process might be far more complex in terms of security, underlying algorithm as well as performance level. Whatever is the level of complexity, the introduction of third party authentication and identity management specialist into any cloud architecture should have only one goal; and the goal is to strengthen the robustness of security in the concerned area which the cloud service provider itself is not capable of to deploy or offer.

## 4. SECURITY ISSUES IN CLOUD

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success (Khorshed, Ali & Wasimi, 2012). The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security (Teneyuca, 2011). Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Cloud users' personal data security is thus a crucial concern in a cloud computing environment (Joint, Baker & Eccles, 2009; Ismail, 2011; King & Raja, 2012). In terms of customers' personal or business data security, the strategic policies of the cloud providers are of highest significance (Joint & Baker, 2011) as the technical security solely is not adequate to address the problem. Trust is another problem which raises security concerns to use cloud service (Ryan & Falvy, 2012) for the reason that it is directly related to the credibility and authenticity of the cloud service providers. Trust establishment might become the key to establish a successful cloud computing environment. The provision of trust model is essential in cloud computing as this is a common interest area for all stakeholders for any given cloud computing scenario. Trust in cloud might be dependent on a number of factors among which some are automation management, human factors, processes and policies (Abbadi & Martin, 2011). Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent. All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud based services – some threats in this category are man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure (Dou, Chen & Chen, 2013). The well known DDoS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this. The security of virtual machine will define the integrity and level of security of a cloud environment to greater extent (Rakhmi, Sahoo & Mehfuz, 2013; Agarwal & Agarwal, 2011). Accounting & authentication as well as using encryption falls within the practice of safe computing - they can be well considered as part of security concerns for cloud computing (Lee, 2012; Ogigau-Neamtiu, 2012; Singh & Jangwal, 2012). However, it is important to distinguish between risk and security concerns in this regard. For example, vendor lock-in might be considered as one of the possible risks in cloud based services which do not essentially have to be related to security aspects. On the contrary, using specific type of operating system (e.g. open-source vs. proprietary) might pose security threat and concerns which, of course, is a security risk. Other examples of business risks of cloud computing could be licensing issues, service unavailability, provider's business discontinuity that do not fall within the security concerns from a technical viewpoint. Thus, in cloud computing context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing (Ogigau-Neamtiu, 2012). Any security tools or other kinds of software

used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment (Bisong & Rahman, 2011; Singh & Jangwal, 2012).

As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach (Bisong & Rahman, 2011). The approach by which cloud computing is done has made it prone to both information security and network security issues (Rakhmi, Sahoo & Mehfuz, 2013; Qaisar & Khawaja, 2012). Third party relationship might emerge as a risk for cloud environment along with other security threats inherent in infrastructural and virtual machine aspects (Hashizume et al., 2013). Factors like software bugs, social engineering, human errors make the security for cloud a dynamically challenging one (Kim, 2009). Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment (Westphall et al., 2011).

The facets from which the security threat might be introduced into a cloud environment are numerous ranging from database, virtual servers, and network to operating systems, load balancing, memory management and concurrency control (Hamlen et al., 2010). Data segregation and session hijacking are two potential and unavoidable security threats for cloud users. One of the challenges for cloud computing is in its level of abstraction as well as dynamism in scalability which results in poorly defined security or infrastructural boundary. Privacy and its underlying concept might significantly vary in different regions and thus it may lead to security breach for cloud services in specific contexts and scenarios (Chen & Zhao, 2012). Data loss and various botnets can come into action to breach security of cloud servers. Besides, multi-tenancy model is also an aspect that needs to be given attention (Kuyoro et al., 2011; Ogigau-Neamtiu, 2012) when it comes to security. Security in the data-centres of cloud providers are also within the interests of security issues, as a single physical server would hold many clients' data (Okuhara, Shiozaki & Suzuki, 2010) making it a common shared platform in terms of physical server or operating system. The storage security at the cloud service providers data centres are also directly linked with the security of the cloud services (Mircea, 2012). All the traditional security risks are thus applicable with added degree of potency in a cloud infrastructure which makes the ongoing success of cloud computing a quite challenging one. Confidentiality, availability and integrity are the generalized categories into which the security concerns of a cloud environment falls. Threats for a cloud infrastructure are applicable both to data and infrastructure (Agarwal & Agarwal, 2011).

Different modes of data transfer and communication means (e.g. satellite communication) might need to take into account. Huge amount of data transfer is a common anticipation in a cloud environment, the communication technology used along with the security concerns of the adapted communication technology also becomes a security concern for the cloud computing approach. The broadcast nature of some communication technology is a core concern in this regard (Celesti, Fazio, Villari & Puliafito, 2012). Cloud environment is associated with both physical and virtual resources and they pose different level of security issues – having no sophisticated authentication mechanism to fully address the security threats is an existing problem for cloud computing. It has mainly resulted in the situations where grid computing has been taken as an embedded part of cloud computing (Casola, Cuomo, Rak & Villano, 2013). As the virtualized resources are highly coupled with a cloud infrastructure, intrusion related security concerns are of utmost priority as part of security issues. Arbitrary intermittent intrusion needs to be monitored in the operational context of a cloud computing infrastructure where the severity of possibility for a virtual machine

to be compromised is to be taken into account (Arshad, Townsend & Xu, 2013). Some authors have argued that using Internet technologies is not a must for cloud computing (Khorshed et al., 2012) - but the cost efficiency and globalization trends will enforce and motivate almost all the businesses to admit Internet and associated technologies to be the ultimate means towards cloud computing approach. As a result, total Internet related security concerns are anticipated to be automatically added on top of the cloud-specific security issues. Bringing portability is one of the means to make cloud services flexible. The portability of cloud services would also be associated with security concerns. Cloud portability enables the cloud users to switch among different cloud service providers without being affected with the necessity to change the ways to accomplish tasks in different ways. It is a clear provision on bargaining power for the cloud users; but at the same time, the security issues with cloud portability are to be counted. Cloud portability might bring severe degree of API based security threats (Petcu, Macariu, Panica & Craciun, 2013).

The wide transition to mobile computing practices in recent years has made it imperative to include mobile computing and its associated technologies as an essential part of cloud computing. Resource scarcity as well as other constraints of mobile computing is barriers to cloud computing. The demand of huge data processing is a problem for mobile end-user devices which has been further complemented by the security concerns of mobile cloud computing. For mobile cloud computing, the device level limitations has inspired researchers to suggest the inclusion of another level of cloud termed as 'mobile cloud' to aid the processing of the specific computing and processing for mobile computing devices (Fernando, Loke & Rahayu, 2013). The earlier explained broadcast nature of satellite communication and related security issues are equally applicable to the mobile cloud computing due to its being wireless communication. Besides, the addition of mobile cloud into the perspective would add another cloud with all its security issues for a service provider having both mobile cloud and conventional cloud. The addition of mobile cloud in the scenario would boost performance, but it would also add another layer of security issue not only to the mobile cloud users, but also to the total infrastructure of the cloud service provider. The hierarchical arrangement of cloud computing facilitates different level of extensibility for the cloud users with varying degree of associated security issues (Che et al., 2011). Security issues for cloud computing are described by some authors as an obvious one due to its nature. In a business model, the risks for the consumers are related to and dependent on the relevant approaches and policies of the cloud service providers the consumers are dealing with. Using cloud products or services may lead to security concerns for the consumers if they are not well aware with the type and particulars of the products or services they are to procure or to use in a cloud environment; this is also related to the cloud providers' identity and reliability. One of the inherent problems in this context is that, the consumers might normally not be able to identify or foresee all the risks involved in the specific cloud transaction they are dealing with or involved in (Svantesson & Clarke, 2010).

## 5. CONCLUSIONS

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is a great opportunity and lucrative option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The vast possibilities of cloud computing cannot be ignored solely for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect could infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer (Dukaric & Juric, 2013). Security for cloud computing environment is a non-compromising requirement. Cloud computing is inevitable to become the ideal (and possibly the ultimate) approach to business computing though the security barriers along with other issues need to be resolved for cloud computing to

make it more viable (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011) . Yet, given its total advantages and dynamism and provided it is deployed within an integrated and secured infrastructural framework, cloud computing can offer virtual ownership and access to 'super computers' without procuring them physically. Perhaps this is what inspired coining the term SCC (Scientific Cloud Computing). Research effort has been contributed to develop faster yet secured SCC tools (Jorissen, Villa & Rehr, 2012) which will greatly influence the pace of research and motivation in various fields together with clouding computing itself. The social implications of cloud computing approaches might emerge with severe impact if robust security models for cloud computing do not exist. The security issues for cloud computing are not related to the technical and direct security breach only; a number of social inconsistency might also be resulted even without any 'hard' security breach having taken place. The distributed and dispersive processing, transmission and storage features are behind reason. One such example is the obtaining of digital evidences. The evolution of cloud computing might significantly affect the collection and retention of digital evidence (Mason & George, 2011). The vastness and potentiality of cloud computing cannot be overlooked, subsequently robust security models for cloud computing scenarios is the most prioritized factor for a successful cloud based infrastructure development and deployment. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements that from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users' and the cloud service providers' ends. The security issues in cloud computing are somewhat sensitive and crucial on the basis of sociological and technological viewpoints – the technological inconsistency that results in security breach in cloud computing might lead to significant sociological impacts. As a result, when dealing with cloud computing and its security issues, technical as well as epistemological factors are equally important to take into consideration. Based on the fact that the impact of cloud computing can include both the technical and social settings, the research on cloud computing and its related concerns are not related only with computing aspects. Service oriented architecture and other characteristics of cloud computing suggests that the concept of cloud computing would require to analyze the practicality in line with social, business, technical and legal perspectives – all these facets will incorporate security issues either in technical or strategic form. Regardless of the nature of security issues, it can be undoubtedly concluded that the severe adverse effects as a consequence of security breaches in cloud computing, the deployment of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems.

# REFERENCES

[1]  Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006

[2]  Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.

[3]  Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009

[4]  Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.

[5]  Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103

[6]  Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.

[7]     Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future.2011.08.008

[8]     Celesti, A., Fazio, M., Villari, M. and  Puliafito, A. (2012). Virtual machine provisioning through satellite communications in federated Cloud environments. Future Generation Computer Systems, 28, 85–93. doi:10.1016/j.future.2011.05.021

[9]     Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551

[10]    Chen, D. and Zhao, H. (2012).  Data Security and Privacy Protection Issues in  Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193

[11]    Dou, W., Chen, Q. and Chen, J. (2013). A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems, 29, 1838–1850. doi:10.1016/j.future.2012.12.011

[12]    Dukaric, R. and Juric, M.B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29, 1196–1210. doi:10.1016/j.future.2012.09.006

[13]    Emam, A.H.M. (2013). Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.

[14]    Fernando, N., Loke, S.W. and Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29, 84–106. doi:10.1016/j.future.2012.05.023

[15]    Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Naslund, M. and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing, 1(11), 1-18.

[16]    Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 39-51. doi: 10.4018/jisp.2010040103

[17]    Han, J., Susilo, W. and Mu, Y. (2013). Identity-based data storage in cloud computing. Future Generation Computer Systems, 29, 673–681. doi:10.1016/j.future.2012.07.010

[18]    Hashizume et al. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5), 1-13.

[19]    Ismail, N. (2011).Cursing the Cloud (or) Controlling the Cloud? Computer Law & Security Review, 27, 250 – 257. doi:10.1016/j.clsr.2011.03.005

[20]    Joint, A. and Baker, E. (2011). Knowing the past to understand the present 1 e issues in the contracting for cloud based services. Computer Law & Security Review, 27, 407 - 415. doi:10.1016/j.clsr.2011.05.002

[21]    Joint, A., Baker, E. and Eccles, E. (2009). Hey, you, get off of that cloud? Computer Law & Security Review, 25, 270–274. doi:10.1016/j.clsr.2009.03.001

[22]    Jorissen, K., Villa, F.D. and Rehr, J.J. (2012). A high performance scientific cloud computing environment for materials simulations. Computer Physics Communications, 183, 1911–1919. doi:10.1016/j.cpc.2012.04.010

[23]    Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 28, 833–851. doi:10.1016/j.future.2012.01.006

[24]    Kim, J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151-160.

[25]    Kim, W. (2009). Cloud Computing: Today and Tomorrow. Journal of Object technology, 8(1), 65-72.

[26]    King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.

[27]    Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science, 1(2), 53-58.

[28]    Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks, 3(5), 247-255.

[29]    Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.

[30]    Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011).Cloud computing — The business perspective. Decision Support Systems, 51, 176–189. doi:10.1016/j.dss.2010.12.006

[31]    Mason, S. and George, E. (2011). Digital evidence and 'cloud' computing. Computer Law & Security Review, 27, 524-528. doi:10.1016/j.clsr.2011.07.005

[32]  Mircea, M. (2012). Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology, 66, 539-546.

[33]  Mosher, R, (2011). Cloud Computing Risks. ISSA Journal, July Issue, 34-38.

[34]  Ogigau-Neamtiu, F. (2012). Cloud Computing Security Issues. Journal of Defense Resource Management, 3(2), 141-148.

[35]  Okuhara, M., Shiozaki, T. and Suzuki, T. (2010). Security Architectures for Cloud Computing. FUJITSU Science Technology Journal, 46(4), 397–402.

[36]  Petcu, D., Macariu, G., Panica, S. and Crăciun, C. (2013). Portable Cloud applications—From theory to practice. Future Generation Computer Systems, 29, 1417–1430. doi:10.1016/j.future.2012.01.009

[37]  Petre, R. (2012). Data mining in Cloud Computing. Database Systems Journal, 3(3), 67-71.

[38]  Qaisar, S. and Khawaja, K.F. (2012). Cloud Computing: Network/Security Threats and Countermeasures. Interdisciplinary Journal of Contemporary Research in Business, 3(9), 1323-1329.

[39]  Rashmi, Sahoo, G. and Mehfuz, S. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401

[40]  Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, 513-521. http://dx.doi.org/10.1016/j.clsr.2012.07.002

[41]  Sharma, S. And Mittal, U. (2013). Comparative Analysis of Various Authentication Techniques in Cloud Computing. International Journal of Innovative Research in Science, Engineering and Technology, 2(4), 994-998.

[42]  Singh, S. and Jangwal, T. (2012). Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues. International Journal of Computer Science & Information Technology, 4(2), 17-31.

[43]  Svantesson, D. And Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, 26, 391-397. doi:10.1016/j.clsr.2010.05.005

[44]  Suresh, K.S. and Prasad, K.V. (2012). Security Issues and Security Algorithms in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 2(10), 110-114.

[45]  Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16, 102-107. doi:10.1016/j.istr.2011.08.005

[46]  Westphall, C.B., Westphall, C.M., Koch, F.L., Rolim, C.O., Vieira, K.M., Schulter, A., Chaves, S.A., Werner, J., Mendes, R.S., Brinhosa, R.B., Geronimo, G.A. and Freitas, R.R. (2011). Management and Security for Grid, Cloud and Cognitive Networks. Revista de Sistemas de Informação da FSMA, 8, 8-21.

[47]  Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D. (2012). Efficient Password-based Two Factors Authentication in Cloud Computing. International Journal of Security and Its Applications, 6(2), 143-148.

[48]  Youssef, A.E. (2012). Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6), 838-847.

[49]  Zissis, D and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28, 583–592. doi:10.1016/j.future.2010.12.006

**Authors**

**Monjur Ahmed** achieved MSc in Electronics and Communications Engineering from University of Greenwich, United Kingdom, MS in Telecommunications from University of Information Technology & Sciences, Bangladesh, and BSc (Hons) in Computing and Information Systems from London Metropolitan University, United Kingdom. He currently serves as Senior Lecturer at Daffodil Institute of IT, Bangladesh. Ahmed's research interests are within communication network performance and cloud computing with a specific focus on security aspects of cloud computing. Epistemological analysis in Information Engineering is also part of his research interests.

**Mohammad Ashraf Hossain** achieved BSc (Hons) in Computing and Information Systems from London Metropolitan University, United Kingdom. He works as freelance IT consultant on cloud based services. His expertise falls within the tools for both private and public cloud. The cloud based tools that he works with are Microsoft Office 365 (SharePoint, Exchange, Lync), Windows Azure 2, Hyper-V and System center. Hossain's research interest is in the area of could based services. He has an interest to study on how the identity management in the cloud based computing approach can be achieved in a secured and integrated way.