Addressing Security and Privacy Issues in Cloud Computing

Yousef K. Sinjilawi, Mohammad Q. AL-Nabhan and Emad A. Abu-Shanab
Faculty of Information Technology and Computer Science
Yarmouk University, Irbid, Jordan
josseph_hfs@hotmail.com, mq_nabhan@hotmail.com, abushanab@yu.edu.jo

Abstract—**Cloud computing is a new development of grid, parallel, and distributed computing with visualization techniques. It is changing the IT industry in a prominent way. Cloud computing has grown due to its advantages like storage capacity, resources pooling and multi-tenancy. On the other hand, the cloud is an open environment and since all the services are offered over the Internet, there is a great deal of uncertainty about security and privacy at various levels. This paper aims to address security and privacy issues threatening the cloud computing adoption by end users. Cloud providers are mindful of cloud security and privacy issues and are working hardly to address them. Few of these threats have been addressed, but many more threats still unsolved. This paper focused on cloud computing security and privacy threats, challenges, and issues. Furthermore, some of the countermeasures to these threats will be discussed and synthesized. Finally, possible solutions for each type of threats will be introduced before we end with conclusions and future work.**

Index Terms—**Cloud computing, architecture, security issues, privacy issues, challenges, solution methods, privacy laws, privacy challenges, security challenges.**

I INTRODUCTION

As the Internet grew more popular, many new technologies such as a cloud computing appeared and caught the attention of many industries. Cloud computing (CC) became popular because of its unique features like dynamic massive scalability, elasticity, measured service and self-provisioning of resources, convenient and on-demand network access, and a shared pool of resources. This means that the cloud is an open and shared environment, which makes the privacy and security of users' data a complex issue. CC exhibits a lot of security threats like sensitive data loss, cloning and data leakage. The cloud providers are mindful of the cloud security and privacy issues and are working on addressing them.

Only few of those threats have been addressed, but many more threats still unsolved. Security is one of the most significant challenges that face the cloud, and privacy makes the cloud more complex to maintain [1]. When we think about the benefits of cloud computing which revolves around sharing resources, information and applications by computer devices connected to the cloud. CC aims to produce a super computer from many normal computers; having more powerful computation capabilities with lowest cost creates a strong cloud [2].

This paper will focus on the major security and privacy issues in cloud computing. Furthermore, it shows the corresponding countermeasures of these issues. The rest of the paper will be organized as the following: The next section summarizes work related to security threats and their solution, followed by privacy concerns and their solutions. Finally, conclusions and future work will be depicted at the end.

II AN OVERVIEW OF CLOUD COMPUTING

Many benefits are gained from using cloud computing, but it also has a lot of threats and issues [3]. The following review will try to understand the concept of cloud computing (CC), explore security and privacy issues, and provide solutions for them.

Nowadays, the cloud is commonly used by various users as they can easily connect using web service or web browsers. CC is characterized by its dynamic infrastructures, global access, massive scalability, fine grain pricing, standard platforms, and management services. It also provides high level services and produces new directions and trends in the IT sector with low cost and low IT resource complexity [4]. The owner of the infrastructure (third party) has the responsibility of service delivery to the users and the maintenance of the infrastructure [5]. Furthermore, it allows gaining flexibility, providing sophisticated services and avoiding software/hardware investment paid up front [1]. Maintaining the data, applications, and the remote servers over the Internet are the main cloud computing features [6].

Ref. [7] introduced a specific platform for each type of the cloud. The authors stated that the AbiCloud platform is used to build private or public cloud in homogenous environment. It's characterized by managing and deploying the servers easily. The Eucalyptus platform is a private cloud with open-source platform and flexible structure that is used to connect a useful system with the users. It's applicable with the applications that need minimum extensions and modifications. Nimbus platform is a solution for cloud computing and an open tool that provides IaaS (infrastructure as a service) using virtual

doi:10.4304/jetwi.6.2.192-199

machine deployment to allow the user to access remote resources and built environment of the required cloud. To allow using the physical resources to manage and/or deploy virtual machine and synchronize the network the open-nebula platform is being used.

Researchers described a new type of cloud called "Community cloud," where it mixes one or more of the hybrid, private or public clouds [8]. This type is shared by various organizations to guard for security issues. Usually, this type of cloud model is managed internally or by third party. The public cloud is more expensive (costly) than the community cloud, while the cost of the private cloud is less than the community cloud.

Others presented the three main service models of cloud computing (business models): IaaS (infrastructure as a service), PaaS (platform as a service) and SaaS (software as a service) [2]. IaaS is the model used when the user can get his service through the Internet from full computer infrastructure, the most popular example of IasS is Amazon EC2. Ref. [1] declared that the IaaS major concern is to build the cloud with a trusted environment and secured information.

PaaS is a model where development, testing and deployment of software can be operated on this platform. PaaS is targeted to developers, administrators and testers. It is considered as a full development environment .Google-Gc engine supports this type of service [2]. SaaS is the most popular form of cloud computing, where the service providers have the full responsibilities for updating, deployment, security, and maintaining the application and they have the administrative control. The combination between Gmail, Google and users is an example of a SaaS model, where the Gmail is software as service provided by Google to the users [2].

Finally, a new business model called DaaS (data as a service) has been introduced, where the visualized storage delivery separates the data storage service and cloud service [7]. It's a special type of IaaS; allowing the client to pay only for the used parts rather than paying for the entire data base (site license). DaaS has been used with the applications that retrieve a huge amount of data with very small timeframe, like: apache Hbase, Google big-table and the Amazon S3.

III Security of Cloud Computing

The cloud as a social infrastructure is the fact that makes security a critical problem [3]. The main drawback of the cloud is building a secure environment for the implementation, business software's, web management and email service offered by cloud computing. It provides enormous potential for a reliable, available, and agile infrastructure in an autonomic, distributed and grid computing environments [9]. On the other hand, the users became edgy and thrilled by cloud computing, its advantages and opportunities, and they are also troubled by security concerns related to implementing it [10].

The cloud providers are aware of the cloud security issues, where it turned into a competitive factor for CC providers. Using a trusted network and platform may improve the cloud security and storage [1]. In order to enhance the service provider's performance, the service security must be guaranteed. A secure cloud provides a reliable service by protecting data and its services available to the client with high performance. Also, it can detect the malicious attacks on the data and service. Furthermore, providers must provide a service free of any problems like data loss or theft problems. Also, the malicious users can access the cloud by embodying legal user, thus may infect the cloud and affect customers by sharing bad and stomachic cloud [11].

A. *The cloud Security Challenges*

Generally, the CC provider must make available a highly secure infrastructure and applications to keep users' data secured from unauthorized access by taking some of the security measures. Some of the cloud computing challenges discussed below and summarized from available literature [5] [7] [10]:

Security: it plays the most important role in cloud computing acceptance prevention, users can't imagine putting their information and running their software on external hard disk and someone else's CPU, these dreading too many. Several security issues like phishing and data loss produce serious threats to data and software operated by the organization.

Costing model: moving toward cloud computing environment generates tradeoffs between integrations and communication costs. CC may reduce the cost of infrastructure but it may increase data communication cost. Such issue can be notable if the user uses the combination of private and public cloud deployment (hybrid cloud) where the resources are distributed among a number of private and public clouds.

Charging model: The cost analysis of elastic resource collection is more complicated than the traditional data center, where the cost is computed based on static computing consumption. Also, the virtual machine is going to become a unit cost rather than physical server analysis item. Strategic charging is critical for profitability and sustainability of the SaaS providers.

SLA (Service Level Agreement): The user doesn't have full control over the resources in the cloud, but when migrating to the cloud, they need to ensure the reliability, performance, availability and the quality of the resources provided by CC service providers. This will be done using SLA. SLA contains levels of granularity, expressiveness vs. complicatedness, and tradeoffs for covering the user needs and expectations.

The advanced SLA approach depends on user's feedback regarding two major issues: What to migrate? And Cloud interoperability. Resources and processes that can be migrated to the cloud can range from the IT management, business applications, server capacity, application level and the application deployment. But, when migrating business data, security and privacy issues need to be addressed. The second issue is interoperability, where different clouds have different ways of users/client interactions with the cloud. Interoperability aims to recognize the seamless flow of data across clouds and between local applications and the cloud.

Other authors [12] classified the security challenges depending on the cloud type, which is an important issue when considering adopting certain type of cloud. Table 1 is a summary of their work.

TABLE 1
CLASSIFICATION OF SECURITY CONCERNS ACCORDING ON CLOUD TYPE

Personal Cloud	*General Cloud*
-Identity and access management. -Data protection. -Security intelligence. -Software, platform & infrastructure security.	-DOS attack. -Attack on virtual machine. -Placing malicious code. -Attack on physical machine.
Domain-Specific Cloud	*Mixed cloud*
-Compliance and auditing. -Firewall feature & -Intrusion detection. -Access controls -Antimalware & antivirus protection.	-Multiple cloud tenants -Ongoing compliance concern.. -Identity management & access control. -Data slinging.

Since the personal cloud has been developed in order to improve the architecture efficiency by providing applications for emails, online collaboration, and calendaring such as ERP software, it may face several types of security issues. The following are some of these issues: security intelligence, data protection and identity management. On the other hand, the general cloud has more significance and unsolved security concerns because of the shared services and infrastructures, those concerns include: VM attack, DOS attack, and putting malicious code and the physical machine attack. Also, the clouds that have been used for specific purposes can face some of security concerns which is related to financial services, management tools, and IT assets. Examples of these concerns are: auditing, compliance, firewall feature. Finally, the hybrid cloud is a combination of one or more of general cloud with one or more private cloud; it faces other types of security concerns such as: Data slinging, identity management, risk that introduced from the multiple tenants of the cloud, and ongoing compliance [12].

Another security challenges' classification is based on the service and deployment of the cloud computing models and it also shows the network issues [10]. The authors discussed various types of concerns which relate to the deployment model like: Resource/cloning pooling, multi-tenant environment sharing, elastic perimeter, data residuals and motility of data, identity management, and unencrypted data. Also, some of the major security challenges that relate to the service model has been discussed; these challenges are the following: consequent problems/data linkage, shared technological issues, VM hopping, malicious attacks, service hijacking, VM mobility, backup and storage. Furthermore, they discussed the security challenges that maybe introduced from the network itself, these issues are the browser security, flooding attacks, locks in, incomplete data deletion, the Signature Wrapping of XML, and injection attack of SQL.

B. The Cloud Security Issues

The literature contained many classifications and typologies of CC security issues, where researchers and practitioners described these issues from diverse views. Ref. [2] classified cloud computing security issues into two main categories: security issues faced by the providers and security issues faced by the users. Security issues are holding back the growth of CC market. Some companies are returning back to their own platforms because they don't need to be exposed to security risks [7]. Also, others defined the main cloud security issues as follows: wrapping XML signature, Browser Security, Cloud middleware attacks, and Flooding attacks [6].

The attacks that may affect the web service can also affect cloud computing due to the fact that the user uses web services and web browsers in order to connect to the cloud. One of the well-known attacks is wrapping XML signature for web service, while the XML signature had been used by WS-security in order to protect the elements name, values and its attributes from unauthorized parties. Attackers can produce malicious messages (by editing the SOAP message by inserting a value and copying the target elements the send the original message to another destination) that can be addressed by using XML signature with WS-Security.

Browser security is that attack when users send a message, they must wait a cloud server to complete the computational processes, before this request, the client must be authenticated to use the cloud system. These can be done with the SSL/TLS process, where the browser has to use it in order to encrypt the cardinalities and uses hand shake 4-ways to authenticate the clients. When the attacker starts sniffing the package, he can use the cloud as an authorized user, for handling this issue, WS-security on the message level is implemented.

Cloud malware attack (CMIA) happens when the attacker creates his own application (a malicious application) on a virtual machine, then it's added to the cloud and considered as valid instance. The malicious instance executed after the client requests it. To handle this type of attack, the service integrity test is conducted. Finally, Flooding attack is the consuming of all of the computational resources by producing workloads through providing instances of service in order to release extra requests (DOS attack). The intrusion detection system and firewall are used to reduce the effect of flooding attacks.

Ref. [8] identified another cloud security issue called data protection. The data is protected when one customer data is separated from the other customers; it must be securely saved/transmitted preventing any third party to access it. Incomplete data deletion, where it's impossible to remove the cloud services accurately, because when the client request the data deletion, copies of the data stored in the nearest replicas but not available in the deletion process. Virtualized private cloud is a countermeasure that is used to remove the complete data from all replicas with its server. Lock –In, which is understanding service, data, application portability by service edge and standard process may prevent the client change the providers or return the service back to IT-Home location. The authors also identified other security issues like: denial of service, network sniffing, port scanning, SQL injection attack, and site scripting [8]. The following are five key security issues with their suggested solutions [9]:

1. Authentication: when unauthorized users access the service and users' information, the identity management system must be applied.
2. Access control: using SLA with access control to identify only the authorized users of the cloud.
3. Policy integration: access different cloud providers by different nodes may raise a conflict between their policies; hence, a solution is needed to work out the inconsistencies between those policies.
4. Service management: composed service by many cloud providers produced to meet customers' needs, thus needs a service integrator to get accurate service.
5. Trust management: the approach of trust management should be used as the negotiation factor of the users and provider of the cloud. Some level of trust must exist interchangeably between cloud providers and users.

Several security issues can affect the cloud security levels, the following are a short list of these [3] [7] [9]:

Privileged user access: Processing sensitive data outside the enterprise faces the risk of logical, physical and personnel control.

o Regularity compliance: Even when the data is held by the providers, the clients have the responsibility of their data security and integrity.
o Recovery: When the cloud server is down, what will happen to the client data? Can it be restored easily? Clients don't prefer to let go their data control to a third party.
o Viability: The availability of the data after faults (provider's faults) or go-broke taking a place in the clients thinking.
o Data segregation: Data from customers share the same environment with other customers' data, using encryption is efficient but is it enough?
o Data location: When moving to cloud computing, clients will not know where their data is stored, because the cloud uses distributed storages for hosting the data. Such issue decreases data control by its owner. Is this acceptable by the client?
o Investigative support: Investigating service of the cloud is difficult because multiple customers' logging to their data is spread and collected via a set of data centers/servers.

C. *Solutions to Security Issues*

Many security issues such as data segregation, authentication, privacy, policy integration, console security, recovery, and access sensitive data, may face cloud computing. To handle those threats, some solutions like API standardization, legal support improvement, virtual machine improvement, and cryptography have been used [9].

To reach an acceptable level of security in the cloud, it's important to have standard security measures. Ref. [4] focused on the measures of the security that are used to increase the effectiveness of cloud computing implementation. These proposed measures were the following: encryption, efficient data storage, visualization using a distributed file system.

The most important requirements that may keep the cloud safe from threats are: availability (resources and services are available for use to users al time), confidentiality (users' data must kept secure using cryptography and data isolation), data integrity (unauthorized users can't modify the data), controls (organize the process of system use of its data, applications and infrastructure), and auditing (seeing what happened in the system during the access duration) [7].

By using the IAM- identity and access management, the cloud will have a robust identity which is useful factor that allows the cloud providers to identify identities. The providers can outsource the identity management by using identity as a service. Also, compliance (programmatic approach to compliance and monitoring) may help the users and the providers to address requirements and the cloud business model [13]. By considering the adoption of "Security as a service" in the cloud security, work will expand to external providers and a lot of security information requirements need to be defined for the organization as required.

Ref. [1] discussed various areas of security concerns: Data at rest, data in transit, incident response, customer separation, authentication and cloud legal issues. They also produced a new paradigm of cloud computing security and information protection; the new trusted model that addresses the main security challenges. By using trusted technologies, security can be improved, which can benefit the clients and the providers. The threats can be classified into 4 categories: A- threats discovered by cloud security-alliance (CSA). B- Threats that concern the location. C- Threats inherit from the network. D- Other threats. Ref. [13] proposed suitable countermeasures for security threats and as shown in Table 2.

Other issues related to cloud security are explored by research [14], where they focused on the process of adopting the cloud concept. Issues discussed include the following: user access, long-term viability, data segregation, disaster recovery and regulatory compliance. There research also suggested solutions for these issues; the following is a summary of these solutions.

Finding an appropriate security management when the cloud has been provided by different vendors may protect the cloud from the major security issues. Also, building a clear contract between the cloud provider and its users is also another solution, while the recovery facilities are being used for retrieving the data completely after losing it. Another solution is by using better enterprise infrastructure; it provides configuration and installation of the components, such as firewalls, routers, operating systems and proxy servers.

TABLE 2
COUNTERMEASURES FOR CSA THREATS

	Forced threat name	Counter measure name
1	Nefarious Use, Confronting Abuse.	Monitor public blacklists, initial registration and validation processes.
2	Malicious Application Interfaces.	Access controls and authentication with encrypted transmission.
3	Malicious Insiders.	Specify resource requirements, compliance reporting, supply chain management.
4	Technology Vulnerabilities.	SLA, security in installation/configuration, monitoring the application environment.
5	Data Leakage /Loss.	Using API access, protecting and encrypting integrity of data, retention strategies.
6	Traffic Hijacking.	Using the user and service account credentials, understanding SLA/ providers' policy.

(Source: summarized from Ashktorab & Taghizadeh, 2012)

Using data encryption also is another solution since no need for further security from the enterprise, and all of the security loads are placed on the cloud provider. The final solution is identifying data flow chart; it allows IT managers to accept the full knowledge about the following issues: Where the data is at each time? Where is it being stored? Where is it being shared?

Finally, the work of Ref. [15] explored various attack types and their definitions. Their work also proposed possible solutions for them. The following are a short list of these common threats in the CC environment: Tampering, information disclosure, repudiation, elevation of privileges, man-in-the-middle, replay attack, identity spoofing, differential analysis threats, and viruses and worms.

IV Privacy Challenges and Issues in Cloud Computing

One of the most important goals we want to achieve in cloud computing security is protecting data privacy. But as we discussed earlier, it is difficult to prevent threats in cloud computing because it is a shared environment that depend on a shared infrastructure. So information will be exposed to the risk of unauthorized access. In other word, we face a big challenge when we talk about sharing a cloud computing resources with protecting customer privacy. The important step to solve this challenge is data isolation, where each customer's information is isolated from other users' information.

Another difficult issue about cloud computing is the movement of data, where data may transfer between countries and face local regulations. Information anonymity is the solution in this case by ensuring customers' data privacy and security [16]. The privacy of users (their identity and data in the cloud) is a very important thing when we talk about cloud computing; and with the growth of cloud computing, the concerns about privacy is also becoming more important [17] [18]. But reaching the peak in providing and assuring privacy data access in cloud computing is still in progress and still needs more attention to achieve users' goals (refer to previous sections and discussions).

One of the biggest challenges for business adoption of cloud computing is the lack of privacy and data security. As discussed earlier, data security risks are potent because of open environment of CC. Such issue raises more challenges related to privacy where it increases the risks of information confidentiality because of the density of data within common clouds. Also, the risk of losing control or governance by organizations when using CC service makes privacy assurance a big concern. Also, one of the main challenges to privacy is the legal issues related to the ambiguous role of cloud service provider and the need for more effective data protection [19].

Another major privacy challenge in cloud computing is the nature of information source; where data and information come from diverse sources. This requires that data be secured and controlled carefully. Also, information should be accessible only to authorized users and not for any user of the cloud, and protected from altering at any time [20]. Privacy of users should be maintained when data is collected, stored or transmitted. The previous conditions mentioned are crucial to the provision of privacy in the cloud and they are: assurance of availability, integrity and confidentiality [16].

The process of data collection from multiple sources as we said above is considered one of the biggest challenges that face cloud computing because it reveals sensitive information about consumers,. Such movement of aggregate data can lead to violating the privacy of users' data [21]. Based on that, customers must be able to acknowledge the access policies to their data and utilities (called access control mechanisms). Furthermore, users' credentials should be defined early in the process and even edited by users when necessary. Finally, identification and authentication between users and the network is important and need to be resolved [22].

After all these issues, we still need to have a proper policy that defines the relations between the major three entities in the cloud: consumers, utilities and third parties involved [16].

To reach an acceptable level of cloud privacy, many issues need to be addressed like: Insufficient user control over his data, information disclosure in movement across the cloud, unauthorized secondary storage of sensitive data, uncontrolled data proliferation, and dynamic provision legal challenges [23].

A. *Privacy Challenges Solutions*

Many methods were proposed to preserve privacy anytime and anywhere. In this review we will describe some of these methods and approaches (called Privacy Preserving Methods). Any approach or technique used must guarantee both preserving the privacy of data as well as assuring data correctness [23].

Anonymity-based Method: The anonymity algorithm works in a very logical manner, firstly, processes the data and anonymizes all or some information before shooting it in the cloud environment. Often not always, the cloud service provider (CSP) uses the background knowledge it has and incorporates the details with the anonymous data to mine the needed knowledge. When studying the traditional approach for privacy preserving (i.e. cryptography technology) we will find that this technique differs from Anonymity-based because Anonymity-based method gets rid of key management and thus it stands simple and flexible. But Anonymity-based method is easier, the attributes that has to be made anonymous varies and it depends on the cloud service provider [23] [24].

Privacy Preserving Authorization System: Users can define their access policies and how to access their data to assure the controlled access of data in the cloud. Policy Decision Points (PDP) and Policy Enforcement Points (PEP) are used for making authorization decisions and enforcing these decisions respectively. Master Policy Decision Points are launched, which figure out and solve the conflicts among various decisions of different PDPs. Obligation service is provided as a part of the authorization infrastructure, by means of which the data owner is informed/stated about authorized or unauthorized access of their data. As the cloud provider is trusted, encryption of outsourced data is not done [25].

Privacy-preserving Architecture: When we talk about architecture we mean the main architectural elements which are user interface, user engine, rule engine and the cloud database [26]. As the cloud architecture has the full responsibility for managing the database storage, which preserves the privacy of users' data. On the other hand, through user interface, the request for accessing database is obtained, and this request is sent as an XML/RPC request to the user engine then to rule engine and finally to cloud database which is responsible for privacy of users. After the request arrives to the database, encryption and assigning secured identities for each request is done. Also, response at each stage with the maintenance of machine readable, and enforcing usage/access rights complete the process of preserving privacy. This approach prevents the risk of both internal and external attacks to outsourced data however this approach faces a big challenge in providing machine readable access rights [23].

Oruta approach: Ref. [27] extended another public auditing mechanism (pervious work of [28]) and analyzed it, then concluded to a new approach called "Oruta" approach to provide a data privacy, identify privacy and also ensure accuracy and lack of fraud while carrying out the public auditing. The previous approaches (proposed by Ref. [28] & [29]) did not reach the privacy identity which is different than this approach. This approach takes into account three major entities: cloud server, third party auditing (TPA) and the users whom are statically grouped into two types: the original users and group users. Original user can control their data and its flow in the cloud so; users request then wait for verification of data depending on TPA to carry out auditing. Here, Three algorithms: KeyGen, RingSign and RingVerify are constructed for achieving the privacy-preserving auditing [23].

B. Privacy Laws and Regulations

Realizing the difficulties facing cloud computing, we must control the cloud using legal constraints, which are important because privacy intrusions on the Web are so prevalent,. These difficulties may result from deregulation of Internet issues (government's responsibility), to sustain an acceptable privacy levels and encourage users to use cloud computing. Also, researchers are worried that could computing concept will jeopardize online advertising industry and other related sectors [30].

Another important issue to be considered when we are dealing with cloud computing environment is the social direction to regulate the domain. There are two main options that can be used: addressing the issues of market and self-regulation or by regulating it by the government. Within the privacy context there are differences between a self-regulation versus the government regulation. Some users believe that government shouldn't control the legal directions in privacy, trying to avoid the standard view of the big brother role of government. Other users proclaimed that self-regulation is difficult as no available mechanism in the CC industry to select educated, significant, and logical policies to implement.

Researchers concluded that regulations don't participate in enforcing an effective Internet practices when dealing with privacy, where market forces might be more influential than regualations in protecting privacy [30]. On the other hand, users considered that rules don't have important impact on privacy only but also could have a negative impact on protecting privacy like decreasing availability of information and increasing transaction costs.

Other directions in research concluded that making the administrative process more efficient and to resolve data privacy issues, cloud regulators need to differentiate personal and non-personal data [31]. The authors suggested a complaints department to handle this issue, where users submit their complaints a service provider, then complaints be forwarded anonymously to public authorities, and finally, run its operations in a public cloud. Public departments need not need to find any additional data about the sender.

V CONCLUSIONS

In this paper we explored the cloud computing environment and tried to discuss security and privacy concerns related to cloud computing. Also, we investigated the different architectures and their requirements, applications and associated challenges and concerns. In this paper we described some models and solutions to create a simplified view of cloud computing and solve some of problems which face businesses in their work.

Security and privacy concerns can be considered a real challenge in this field. Some solutions depended on the level of trust and confidence users possess in the cloud concept or providers. Also, by using SLA, the user can access the cloud securely, thus requires lots of reputation management. The end users are thrilled and edgy by the cloud computing even though cloud computing provides lots of opportunities which made the users so excited, but they are anxious about the security concerns. Research is growing tremendously for the purpose of identifying such challenges and proposing solutions for them. The real question is that: Would the synergies from utilizing the lower cost of cloud computing (economical gains) outweigh the risks associated with its security challenges?

Also, in this work, privacy concerns were identified as an associated concern with security flaws. Privacy issues were discussed and some solutions also were proposed. To achieve privacy goals, we distilled few proposed methods from the literature such as: anonymity-based method, privacy preserving authorization system, privacy-preserving architecture and Oruta. There are much research on ensuring the security of outsourced data in an untrusted cloud data center and how to achieve the privacy of users' data.

This research work focused on providing solutions to address security and privacy concerns and synthesize the literature in this area. The cloud computing concept is a multidimensional one, where many factors determine its success. Businesses are keen on understanding this concept and this is why this paper is crucial to research and practice society. Also, with the financial crises and the tight budgets businesses face, it is vital to search for opportunities to reduce operational cost and reduce the risk of obsolescence of technology.

Future work in this area should focus of two major tracks: the economies of cloud computing and the reality of this concept. The second track is the business adoption of such environment and how top management takes the decision to follow such path or not. The Innovation Diffusion Theory (IDT) is a suitable tool that contributes to understanding the adoption process of organizations. Finally, the security and privacy issues discussed need to be explored empirically through a field research that investigates the perceptions of organizations after adopting cloud computing and how they evaluate such experience.

REFERENCES

[1] Patidar, K., Gupta, M. R., Singh, G., Jain, M. M., & Shrivastava, M. P. (2012). Integrating the Trusted Computing Platform into the Security of Cloud Computing System. *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol. 2(2), pp. 1-5.

[2] Madhavi, K. V., Tamilkodi, R., & Sudha, K. J. (2012). Cloud Computing: Security threats and Counter Measures. International Journal of Research in Computer and Communication technology, IJRCCT, Vol. 1(4), pp. 125-128.

[3] Rani, A. M. G., & Marimuthu, A. (2012). A Study on Cloud Security Issues and challenges. Int.J.Computer Technology & Applications, Vol. 3(1), pp. 344-347.

[4] Kumar, K., Rao, V., & Rao, S. (2012). Cloud Computing: An Analysis of Its Challenges & Cloud Computing: An Analysis of Its Challenges & Security Issues. International Journal of Computer Science and Network (IJCSN) Vol. 1(5), pp. 1-8.

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

[6] Jamil, D., & Zaki, H. (2011). Security issues in cloud computing and countermeasures. International Journal of Engineering Science and Technology (IJEST), 3(4), pp. 2672-2676.

[7] Kumar, S., & Goudar, R. H. (2012). Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication, Vol. 1(4), pp. 356-360.

[8] Qaisar, S., Khawaja, K., (2012). Cloud Computing: network /security threats and countermeasure. Interdisciplinary Journal of Contemporary Research In Business, Vol. 3(9), pp. 1323-1329

[9] Chandrahasan, R. K., Priya, S. S., & Arockiam, L., (2012). Research Challenges and Security Issues in Cloud Computing. International Journal of Computational Intelligence and Information Security, Vol. 3(3), pp. 42-48.

[10] Parekh, D. H., & Sridaran, R. (2013). An Analysis of Security Challenges in Cloud Computing. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4(1), pp. 38-46.

[11] Ashalatha, R. (2012). A survey on security as challenges in cloud computing. International Journal of Advanced Technology & Engineering Research (IJATER), Vol. 2(4), pp. 1-4.

[12] Sharma, M., Bansal, H., & Sharma, A. K., (2012). Cloud Computing: Different Approach & Security Challenge. International Journal of Soft Computing and Engineering (IJSCE), Vol. 2(1), pp. 421-424 .

[13] Ashktorab, V., & Taghizadeh, S. R. (2012). Security Threats and Countermeasures in Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Vol. 1(2), pp. 234-245.

[14] Tiwari, P. K., & Mishra, B. (2012). Cloud Computing Security Issues, Challenges and Solution. International Journal of Emerging Technology and Advanced Engineering, Vol. 2(8), pp. 306-310.

[15] Malik, A., & Nazir, M. (2012). Security Framework for Cloud Computing Environment: A Review. Journal of Emerging Trends in Computing and Information Sciences, Vol.3(3), pp. 390-394.

[16] Younis, Y., Merabti, M. & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep.

[17] Gellman, R. (2013). Privacy in the clouds: risks to privacy and confidentiality from cloud computing. A report published by the World Privacy Forum, Accessed in 2013 from the Internet from: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[18] Xiao, Z., & Xiao, Y. (2013). Security and Privacy in Cloud Computing. IEEE Communications Surveys & Tutorials, Vol. 15(2), pp. 843-859.

[19] Alleweldt, F., Kara, S., Fielder A., Brown, I., Weber, V. & McSpedden-Brown, N. (2012). Cloud Computing. A publication of the European Parliament's Committee on Internal Market and Consumer Protection. Accessed from the Internet in October 2013 from: http://www.europarl.europa.eu/studies

[20] NIST-USA (2010). Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy Architecture, and High-Level Requirements (Vol. 1). A Report published by the National Institute of Standards and Technology, USA.

[21] Rani, S., & Gangal, A. (2012). Security issues of banking adopting the application of cloud computing. International Journal of Information Technology, Vol. 5(2), pp. 243-246.

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

[23] Neela, T. J., & Saravanan, N. (2013). Privacy Preserving Approaches in Cloud: a Survey. Indian Journal of Science and Technology, Vol. 6(5), pp. 4531-4535.

[24] Zhou, M., Mu, Y., Susilo, W., Au, M. H., & Yan, J. (2011). Privacy-preserved access control for cloud computing. Proceedings of the 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE, pp. 83-90.

[25] Chadwick, D., & Fatema, K. (2012). A privacy preserving authorization system for the cloud, Journal of Computer and System Sciences, Vol. 78(5), pp. 1359–1373.

[26] Greveler, U., Justus, B., & Loehr, D. (2011, August). A Privacy Preserving System for Cloud Computing. Proceedings of the 11th International Conference on Computer and Information Technology (CIT), 2011 IEEE, pp. 648-653.

[27] Wang, B., Li, B., & Li, H. (2012). Oruta: Privacy-preserving public auditing for shared data in the cloud. Proceedings of the 5th International Conference on Cloud Computing (CLOUD), 2012 IEEE, pp. 295-302.

[28] Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-preserving public auditing for data storage security in cloud computing. Proceedings of the INFOCOM, IEEE, pp. 1-15.

[29] Wang, C., Chow, S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE Transactions On Computers, Vol. 62(2), February 2013, pp. 362-375.

[30] Kesan, J. P., Hayes, C. M., & Bashir, M. N. (2013). Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency. Wash & Lee L. Rev., Vol. 70(1), pp. 341-472.

[31] Deussen, P., Eckert, K., Strick, L. & Witaszek, D. (2012). Cloud Concepts for the Public Sector in Germany –Use Cases. A publication by Fraunhofer Institute For Open Communication Systems.

Yousef K. Sinjilawi is a computer science lecturer at Tabouk University in KSA. His research interest includes Data mining, Information retrieval, and Cloud computing. He recently graduated from Yarmouk University with Master Degree in Computer Information System (CIS).

Mohammad Q. AL-Nabhan received his B.S. degree in Computer Information Systems from Yarmouk University, Jordan, in June 2012 and M.S. degree in Computer Information Systems from the same University. His research interests include cloud computing, wireless sensor networks, and software testing.

Emad A. Abu-Shanab earned his PhD in business administration, in the MIS area from Southern Illinois University – Carbondale, USA, his MBA from Wilfrid Laurier University in Canada, and his Bachelor in civil engineering from Yarmouk University (YU) in Jordan. He is an associate professor in MIS. His research interest in areas like *E-government, technology acceptance, E-marketing, E-CRM, Digital divide, and E-learning*. Published many articles in journals and conferences, and authored three books in e-government. Dr. Abu-Shanab worked as an assistant dean for students' affairs, quality assurance officer in Oman, and the director of Faculty Development Center at YU.