Security threats and legal issues related to Cloud based solutions

Eesa Alsolami[1]

[1]Information Technology Department, University of Jeddah, Jeddah-Asfan road, Saudi Arabia

Abstract

In present times, cloud computing has emerged rapidly in both public and private sector, it is basically a set of services and resources that are offered to user on a single platform via internet. Although adaptation of cloud computing is yet to reach its full potential, but is widespread adaptation is exponentially increasing throughout the world, some of the well-known cloud service providers are Microsoft and Google. Rapid adaptation of cloud computing had resulted in increasing severity of security and privacy concerns as well as legal challenges. This study includes multiple issues with cloud computing that impairs security and privacy of data, as well as presents on threat that impacts data residing in the cloud. In addition to this, various mitigating approaches for countering these threats are presented hare as well as multiple open issues are noted in this study for further studies for providing a secure cloud computing environment.

Key Words:

Security threats, legal issues, cloud based solutions, Microsoft, Google

1. Introduction

1.1 Cloud Computing: Definition and Features

National Institute of Standards and Technology (NIST) had defined cloud computing as a model that enables universal, easy, on-demand access of network for shared configurable computing resources such as, networks, applications, servers, services and storage, which are provisioned swiftly and are allotted with minimum effort on the part of management or service provider (Kundra, 2011). Five essential features of cloud computing are as follows:

1. On-demand Self-Service: With this feature, users can provision available cloud computing resources such as server time and storage, through a web portal without any human interaction (Healy, 2016).
2. Broad Network Access: Computing resources are available over the network that supports heterogeneous client platforms (Schouten, 2014).
3. Resource pooling: Capability of providing service to multiple customers from same physical resources, by dynamically assigning and reassigning as per consumer demand (Chabrow, 2011).
4. Rapid elasticity: Capabilities are provisioned and assigned as per demand, for consumers application enables unlimited capability it needs at any time (Chabrow, 2011).
5. Measured service: In other words, it is pay per use, cloud systems monitor, measure and bill resource transparently as per utilization (Healy, 2016).

1.2 Security and privacy challenges in Cloud

Multiple security and privacy issues are rising in proportion with the rising popularity of cloud computing, some of them are as follows:

- Data Loss and Breach: It is the most prominent security issue with cloud computing environments this involves loss of data and theft of sensitive/confidential information are few of the concerns here (Sen, no date).
- Lack of Transparency: It is related lack of willingness on the part of Cloud Service Provider to disclose its security measures adopted by the organization (Takabi, Joshi and Ahn, 2010).
- Authentication and Identity Management: It is an interoperability drawback of cloud computing due to identity negotiation protocol and identity tokens (Takabi, Joshi and Ahn, 2010).

2. Need for the study

The growing popularity of cloud computing services is a crucial driver behind converting it into a viable business proposal for reducing the cost of both infrastructure and operations, thus it has become to efficiently manage security and privacy risks in the cloud environment as well as iron out legal issues related to it. In this study, security issues related to cloud computing are discussed along with legal steps undertaken to mitigate such issues. The main motivation behind this study is growing demand for cloud services that are capable, cost effective and secure (Sen, no date). As every organization is constantly searching for new methods of increasing revenue return and decreasing cost, cloud computing platform is a technological development that is essentially reducing the cost of hardware and software service used (Musa and Sani, 2016). There are many cloud service providers in the market namely, Google,

Manuscript received May 5, 2018
Manuscript revised May 20, 2018

Microsoft Salesforce, Amazon and such. They are providing virtual environment with computing resources to meet the demands of an organization and one of the main feature in selecting a cloud service provider is the level of secure access provided by them. Today, users are very careful in selecting their cloud service providers as most of them cannot afford any compromise on security and privacy of data, which is substantial challenge for cloud service provider (Liu et al., 2015). Thus, it is essential to review the security issues faced by cloud service providers and legal implications associated with it.

3. Aim of the study

The main aim of this study is to analyze security threats and legal issues related to Cloud based solutions. This report will discuss security issues with cloud computing, type of attacker, mitigating approaches and legal steps undertaken by various international and national agencies for tackling security issues in cloud-mainly based solutions

4. Central research question

The central research question based on the aim of the study is as follows:
What are the security threats and legal issues related to Cloud computing solutions?

5. Literature Review

Cloud computing is a budding paradigm that tremendous potential to grow and is becoming widely popular, however even with its unique characteristics it has many security and privacy challenges which are discussed in this section of report.

5.1 Threat vectors

The main security concern factors in cloud computing are categorized under confidentiality issues, integrity issues and availability issues and are discussed in brief here:

5.2 Confidentiality Threats

It includes insider threat to user information, threat of external attack and information leakage. First, insider threat to user information, is related to unauthorized or unethical access to user information from insider of cloud service provider is a major security challenge. This threat could originate from malicious cloud service provider user, malicious customer user or malicious third party supporting cloud service provider or customer (Musa and Sani, 2016). Second, threat of external attack, which is more applicable for cloud applications in public domain. This threat includes remote software or hardware attack on cloud application and cloud user, social manipulation of cloud service providers and users and more to retrieve personal data, confidential data and sensitive information. Third, data leakage, which is widespread threat that cloud compromise information due to human error, defective hardware, secure access failure and more (Sen, no date).

5.3 Integrity Threats

It includes threat of data segregation, poor user access control and threat on data quality. First, threat of data segregation, which includes incorrectly definition of security parameters, improper configuration of VMs (Virtual Machines) and incorrect hypervisors. This is a complex issue within the cloud environment, which shares resources between the users and if resources are segregated that could impact on data integrity. Second is poor user access control, which due to inefficient access and identity control protocol that generates many threat opportunities for attackers that can cause damage to data resources(Musa and Sani, 2016). Third is threat to data quality due to faulty hardware component or software application. Sharing of resources amongst multiple user is the reason behind increased risk of impact on data quality that in turn impacts integrity of data in the shared atmosphere(Sen, no date).

5.4 Availability Threats

It includes impact of change management, non-availability of service, physical disruption of resources and inefficient recovery methods. First is impact of change management that includes impact of testing customer penetration on other users and impact of infrastructure changes. Both hardware and software changes within cloud environment have negative impact on availability of cloud services(Musa and Sani, 2016). Second is non-availability of services that include non-availability of network bandwidth, DNS service and computing application and resource. It is an external threat that impacts all cloud models. Third is physical disruption of IT services of service provider, cloud customer and WAN service providers. Resources can be physically disrupted easily by insiders or external attackers in a less secure environments or remote practice. Fourth is weak recovery methods i.e., insufficient disaster recovery protocol, which impact on recovery time and efficiency in case of incident (Sen, no date).

5.5 The threats against information assets residing in cloud computing environments

This section briefly describes security threats for data in cloud computing environment, some of them are as follows:

- Privileged User Access: Cloud service providers usually have limitless access to the information on user for privileged users, that is a potentially high-risk factor that can lead to unethical access to customer data (Jabir et al., 2015).
- Data Segregation and Storage Location: The user data is usually stored at location unknown to user, which poses risk of storing data alongside other customers' data (Jabir et al., 2015).
- Data Deletion: The data not being deleted from the data storage backup or the physical medium used is a high-risk with cloud computing (Jabir et al., 2015).
- Protective monitoring: The consumers have limited ability to invoke their own protective procedures due to complex structure of cloud and had to rely upon cloud service provider for protective monitoring, which is also an invasion to privacy (Axon, 2016).
- Data Leakage and Inconsistency: It usually occurs in cloud when consumers' data is repeatedly stored at multiple data centers for backups. This distributed storage increases probability of data leakage and synchronization failures lead to data inconsistency (Takabi, Joshi and Ahn, 2010).
- Non-Secure Interoperation: Multidomain access control on cloud platform also poses security threat to user information stored in cloud due to interoperation on shared resources, which calls for global policies for mediating all user access and fulfilling all user requirements (Takabi, Joshi and Ahn, 2010).

6. Methodology

Research methodology is a method to scientifically solve the research question or achieve research objectives. It provides understanding of various steps to be adopted while performing any research study(Kothari, 2004). The methodology for this research study was based on systematic review based on security threats and legal issues in cloud-based solutions. The main aim of systematic review is to address research problems by categorizing, critically analysing and integrating all relevant research findings for addressing research questions. A systematic review has summarised the implications made by carefully analysing available literature to make judgements based on evidence and provide suitable recommendations (Siddaway, no date). These reviews are generally complicated as they analyse pool of available data to reach some conclusion. Systematic review is selected for this study as, it provides an understanding on extent of existing literature studies as well as aids in identifying link between research variable, contradictions and gap in existing studies (Cochrane Consumer Network, 2018). In addition to this. it also aids in providing direction for further studies. The systematic review in this research study had revolved around three crucial themes, namely types of attackers and their capability of attacking the cloud, security risks associated with the cloud over the decade (including relevant considerations of attacks and appropriate countermeasures), and mitigating approaches and legal steps taken by international and national agencies to tackle security threats in cloud solutions. These themes are discussed in the following section of report.

7. Discussion

7.1 The types of attackers and their capability of attacking the cloud.

Most of the security issues and privacy challenges in cloud computing environment, that results from attackers that are mainly divided into two broad categories namely internal attackers and external attackers. Internal attackers could be any employee of the cloud service providing organization or any third party associated with supporting cloud services, or any customer of the services. These internal attackers have privileged limitless access to cloud services, infrastructure and applications used and user information, which depends on their position in organization. They unethically use their privileges, to gain more access or any third party in breaching integrity, confidentiality, and availability of data within the cloud service (TagElsir, babiker and Mustafa, 2015).

Another category is external attacker, who is not an employee at the cloud service provider, third party supporting operations or any customer. These external attackers do not have authorized access for accessing cloud services or customer information or any supporting hardware infrastructure and software applications. These attackers exploit technical loopholes, operational faults, process defects and social vulnerabilities in attacking any cloud service provider, supporting third party organization or customer for gaining more unauthorized access and propagating attacks on the integrity, confidentiality and availability of data within the cloud service (TagElsir, babiker and Mustafa, 2015).

In addition to this, within cloud environment, attackers are divided into four categories capability wise namely, random attackers, weak attackers, strong attackers, and substantial attackers. These categories are formed on the basis of their capability to initiate a successful attack irrespective of the type of threat. First is random attacker, which is most common kind of attackers using simple techniques and tools. Such attackers scan the internet randomly to recognize vulnerable components and deploy well known attack methods that are detected quite easily. Second attackers' category is weak attacker or semi-skilled attackers, who targets any particular servers or any cloud service providers by altering present publicly available software tools or data. The methods used by them are more advanced as compare to random attackers as they alter their attacks with available exploitation tools (Sen, no date).

Third category is strong attackers, who are well-organized, skilled and well-financed groups or individuals that have core hierarchy focusing on targeting specific applications or cloud users. Usually, such group are organized crime group that in particular launch large scale attacks. Last category is substantial attackers, who are motivated attackers and cannot be easily detected by organizations under attack, by law enforcement agencies as well as investigative organizations that handles cybercrime and security. In order to mitigate such threats more intelligence on attacks as well as special resources are required to detect such incidents(Sen, no date).

7.2 Security risks associated with the cloud over the decade (relevant considerations of attacks and countermeasures)

Some of the relevant security issues and incidents with cloud computing in past decade as well as their possible counter measures are presented here in brief:

7.2.1 Data Breaches and Leakage

It is an event when private, protected and sensitive information is stolen or leaked by a third party who is not authorized to see it. This kind of attacks can be targeted or could be a result of human mistake or vulnerabilities of system. These issues mainly impact data which is not intended to be made public, intellectual property, financial information or personal information (Jabir et al., 2015). An incidence of data breach had occurred in 2010, Microsoft faced a breach issue with Business Productivity Online Suite, where unauthorized cloud access was detected in their offline employee address books (Bradford, 2018).

Countermeasure: Such kind of issues are not unique to cloud computing but are still a major cause of concern for the users. For mitigating such issues cloud service providers must implement effective security program by using encryption method or efficient authentication protocol (such as, a combination of password, unique security code or biometric) (Cloud Standards Customer Council, 2017).

7.2.2 System Vulnerabilities

This threat includes exploitation of bugs in the program, poorly configured database, illegal software use and such, it enables attackers to infiltrate into cloud system for stealing data or controlling system or disrupting operations. In addition to this, multi-tenancy in cloud computing and shared pool of resources adds to this issue (Joshi, 2014). An example of this threat was noted in 2016, when confidential data of voters from National Electoral Institute of Mexico was compromised, due to poorly configured database by illegally hosting Amazon cloud server (Bradford, 2018).

Countermeasure: Such attacks can be mitigated by following basic IT processes such as vulnerability scanning, quick update management and a quick response on system threats and such (Cloud Standards Customer Council, 2017).

7.2.3 Unsatisfactory Identity and Access Management

Many of the security issues on cloud are result of lax authentication, poor key management and weak passwords. It is essential for a consumer to know about the secure identification measure used by their cloud service provider. In addition to this, centralization of identities on a solitary repository is also a potentially high risks factor, as it can become an easy target for attackers (Axon, 2016). In 2012 such an issue occurred at LinkedIn when 6 million user passwords were published online by attackers (Bradford, 2018).

Countermeasure: This threat can be mitigated by using multifactor authentication method making it difficult for hacker to use stolen passwords to gain unethical access to data without users' consent (Musa and Sani, 2016).

7.2.4 Account Hacking

This is not a new threat, the methods of attack include fraud, exploitation of software bugs and phishing. With cloud platform, by compromising your credential information attacker can intrude on your every web activity and transaction. It can result into distribution of falsified information, redirecting to illegitimate sites, manipulation of data and such more (Joshi, 2014). Such incident had occurred in 2012, when hackers hacked into 68 million accounts of Dropbox and sold stolen credentials on dark web (Bradford, 2018).

Countermeasure: Common defense protection strategies can contain the damage or possibly mitigate such attacks. Simply by prohibiting sharing of account credentials and using two-factor authentication techniques as well as monitoring account activities for early detection of threats (Musa and Sani, 2016).

7.2.5 Insecure Interfaces and Hardware

Cloud computing service providers uses a set of software user interfaces (UIs), application interfaces and virtual infrastructure that is build up on some hardware. Thus, unsecure or compromised hardware or interfaces can cause accidental and malicious breaches to the security of overall system (Musa and Sani, 2016). An example of this threat was noted in Home Depot in 2014, when an attack had self-checkout lanes for several days before detection, affecting around 56 million credit card numbers (Bradford, 2018).
Countermeasure: Such attacks can be mitigated by focused code reviews and rigorous infiltration testing. Code review will audit the source code of the application or service regularly to ensure security and infiltration testing will determine vulnerabilities of the system (Musa and Sani, 2016).

7.3 Mitigating approaches and legal steps taken by international and national agencies to tackle security threats in cloud solutions

Good security measures are essential for cloud platform like any other IT application, some of the existing solutions for mitigating security threats and privacy issues are as follows:

- Encryption Algorithms: Presently, encryption is a major solution in addressing data privacy issues in the cloud computing environment. With encryption algorithms, confidential data is encrypted and is only accessed by users having encryption keys (Liu et al., 2015).
- Access Control: This method includes authorization, authentication and accounting for providing access to authorized users only making data storage more secure (Takabi, Joshi and Ahn, 2010).
- Continuous Upgrade of System: The security position is boosted with continuous system updating by new patches and service packs equips system with necessary security levels (Suri and Nath, no date).
- Early Detection: Early detection of security vulnerabilities and threats aids in containing it quickly before whole platform is affected. It requires specific actions to be taken in timely manner to mitigate the attack (Suri and Nath, no date).
- Information System Auditing: It basically refers to establishing checks and balances within an organization. It aids in maintaining data integrity while it is stationery as well as in transit (Sen, no date).
- Intervention and Help Desk Services: A quick intervention whenever a threat is detected is essential in mitigating a threat. This requires capability for supporting software applications and infrastructures round the clock. Thus, help desk services are essential in aiding in case of failure and attack (Suri and Nath, no date).
- Centralization of Intelligent Log and Analysis: It is a monitoring solution, which is based on matching and correlating log entries. This analysis aids in establishing security threat index and baseline of counter operations. It is a kind of sophisticated tools, which can be used by security experts for generating early warning (Suri and Nath, no date).
- Secure-Service Provisioning: In order to optimize utilization of resources, it is a common practice amongst cloud service providers to segregate software application services from hardware infrastructure. For this automatic service provisioning is required that securely integrates applications with infrastructure (Takabi, Joshi and Ahn, 2010).
- Trust Management: Trust management is one promising method for addressing security and privacy issues in the cloud computing environment, it is mainly categorized as soft and hard trust management. Soft trust management is related to defining relationship between two parties in performing any action. Hard trust management is an upcoming trend for resolving privacy issues and data integrity issues, as it deals with virtual infrastructure provided to client, which is usually built on non-secure physical hardware (Sen, no date).

As discussed above, maintaining security standard and compliance integrity is a huge concern in cloud computing environment. For alleviating such concerns, many international and national bodies have provided relevant standards for cloud services, some of them are Information Technology Infrastructure Library (ITIL), Open Virtualization Format (OVF) and ISO/IEC 27001/27002.

7.3.1 Information Technology Infrastructure Library (ITIL)

ITIL provides set of guidelines defined as unified, process-based method, in order to manage IT services. ITIL guidelines are applied in almost all type of IT services including cloud services. This agency ensures proper data security measures are implemented at strategic level and operational levels in a planned manner. It provides a methodical approach for security management, some of its advantages includes cost reduction, best practice implementation, better customer satisfaction, improved productivity by enhancing skill set and delivery time. These guidelines break data security in four parts namely, policies, processes, procedures and work instructions (Popović and Hocenski, 2016).

7.3.2 Open Virtualization Format (OVF)

It enables secure, effective and elastic software distribution and facilitatesin providing mobility and independent platform to customers through virtual machines. The security is defined here in terms of data integrity, confidentiality and availability and the security goals include validity, accountability, non-negation and consistency(Popović and Hocenski, 2016).

7.3.3 International Organization for Standardization ISO/IEC 27001/27002

This agency formally defines the compulsory requirements for anydatasecurity management system. This standard is used to indicate appropriatedata security controls, it aids IT organizations in dealing with their basic security requirements, such as, ensuring appropriate security level, applying security baseline and providing secure services(Popović and Hocenski, 2016).

7.4 Establishing Conceptual Model establishing the appropriate mitigating solution

Conceptual framework for appropriate mitigating solution is as follows:

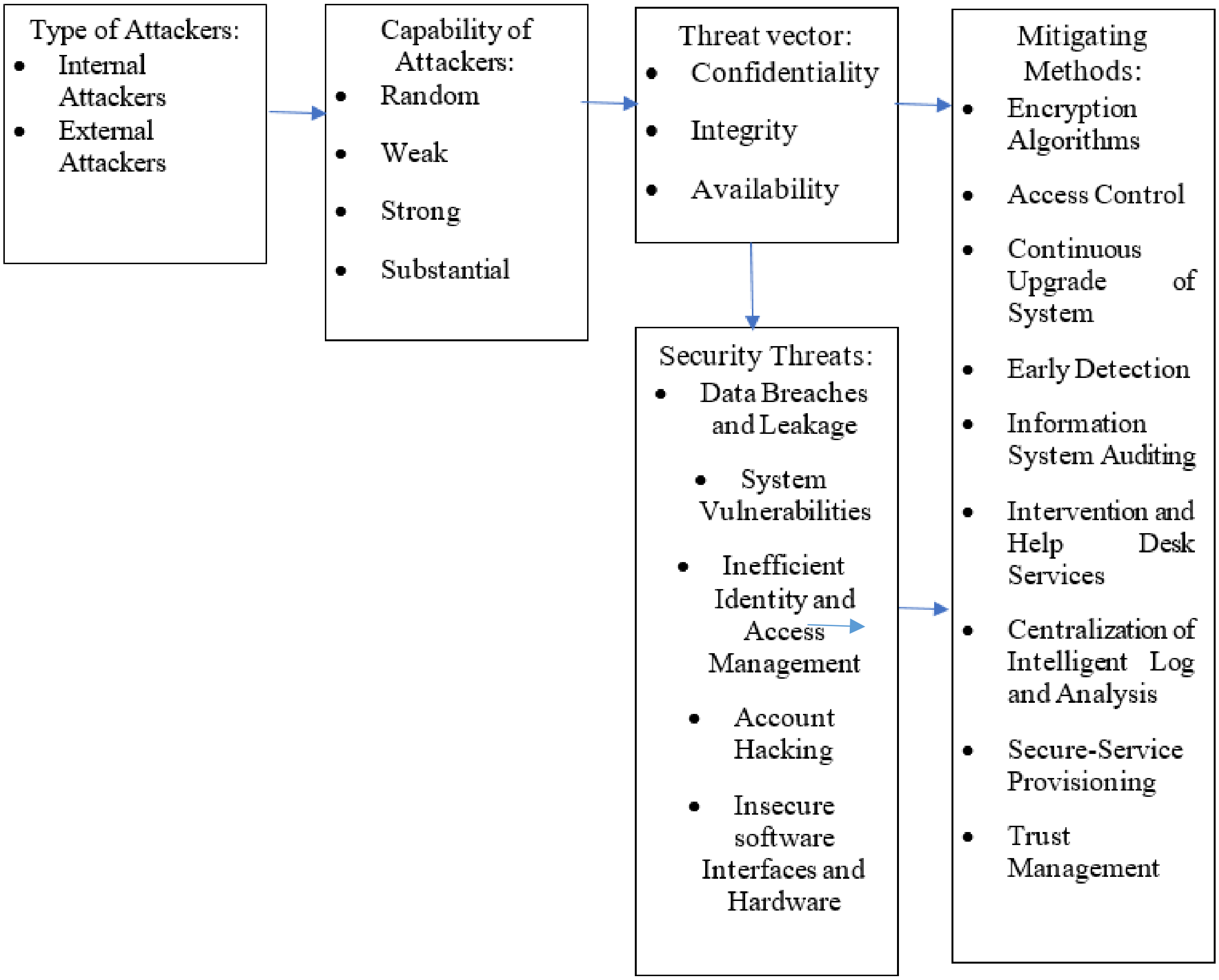

Fig. 1 Conceptual framework for appropriate mitigating solution

8. Conclusion

8.1 Answering Central Question

8.1.1 What are the major security threats and legal issues related to Cloud computing solutions?

As cloud-based solutions are amalgamation of various technologies, such as, virtualization, service-oriented architecture, utility computing and Web 2.0, most of the security issues involved are known problems of IT services casted on a new platform. Major security issues for cloud services are lack of good governance policy, lack of trust, unsecure access to cloud service, permanent loss of data, data leakage, lack of asset management, unsecure infrastructure/hardware, unsecure software interface, unethical access of information by privileged users, information hacking, data segregation, denial of service, shared data storage and malicious external attack (Liu et al., 2015).

Legal challenges that are mostly faced by cloud service provider are, firstly is requirement of multinational framework for privacy and security, which is essential as cloud computing has moved beyond the geographical limits of countries. Development of such framework will aid cloud services to reach their full potential in different countries. Second legal issue is rules of cross border data transfers, as there are many restrictions on such transfers which creates uncertainty and efficiency of could services can be boosted by providing reliable and fast performance. Third main issue is conflicting legal obligations imposed by different governments that puts cloud service providers in a difficult position leading to ambiguity and substantial legal challenges (Suri and Nath, no date).

8.2 Implications

The main concerns with cloud service providers is data security and user privacy protection, this study had discussed various uncertainties and potential security gaps concerning cloud applications and solutions. Thus, it is suggested that accountability of cloud service providers must be increased in matters related to security and privacy breaches, so that appropriate countermeasures are deployed for user data protection. In addition to this, many cloud services providing companies are facing legal conflicts related to jurisdiction of their operation, this impact upon the effective services and performance advantages of cloud computing as well as increasing cost of investment and hindering innovations in this platform. It is recommended to cloud services providers to adopt temporary measures unit a global framework is formed to resolve legal issues.

9. Future Scope

Cloud computing is now a booming trend in IT services, which is dynamically increasing its capacity to match user demands. With increasing cloud capability and number of user, cloud computing security challenges are also increasing which part of many ongoing research studies. There are many open issues, which can be further studied for dealing with security threats. **Further studies can be based on analyzing the method to ensure secure data transfer including encryption and authentication protocol developed for securing** internet traffic. One of the major challenge for security in cloud computing is compromised software interfaces that are used to interact with cloud services exposing multiple security issue that needs further analysis on integrating security services throughout the platform. Another challenge for cloud computing is data segregation, which require more studies to be conducted on the issue of secure data storage. In addition to this, issues like secure user access, hacking, data leakage and lack of quick recovery protocols need more studies to be conducted to completely analyze these challenges.

References

[1] Axon (2016) An introductory paper to the main issues and potential areas for government action Cloud Computing for the Public Sector and its Policy Implications. Available at: https://www.axonpartnersgroup.com/images/Consulting/News/CloudComputing.pdf (Accessed: 13 April 2018).

[2] Bradford, C. (2018) 7 Most Infamous Cloud Security Breaches.

[3] Chabrow, E. (2011) 5 Essential Characteristics of Cloud Computing. Available at: https://www.inforisktoday.com/5-essential-characteristics-cloud-computing-a-4189 (Accessed: 10 April 2018).

[4] Cloud Standards Customer Council (2017) Security for Cloud Computing: Ten Steps to Ensure Success Version 3.0. Available at: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (Accessed: 12 April 2018).

[5] Cochrane Consumer Network (2018) What is a systematic review? | Cochrane Consumer Network. Available at: http://consumers.cochrane.org/what-systematic-review (Accessed: 13 April 2018).

[6] Healy, R. (2016) The 5 Essential Characteristics of Cloud Computing. Available at: https://www.annese.com/characteristics-of-cloud-computing (Accessed: 10 April 2018).

[7] Jabir, R. M. et al. (2015) ‘Analysis of Cloud Computing Attacks and Countermeasures’, ICACT.

[8] Joshi, J. B. D. (2014) ‘Security and Privacy Challenges in Cloud Computing Environments’.

[9] Kothari, C. R. (2004) Research Methodology: Methods and techniques.

[10] Kundra, V. (2011) FEDERAL CLOU D COMPUTING STRATEGY. Available at:

https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf (Accessed: 12 April 2018).

[11] Liu, Y. et al. (2015) 'A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions', Journal of Computing Science and Engineering, 9(3), pp. 119–133. doi: 10.5626/JCSE.2015.9.3.119.

[12] Musa, F. A. and Sani, S. M. (2016) 'Security Threats and Countermeasures In Cloud Computing', International Research Journal of Electronics & Computer Engineering, 24.

[13] Popović, K. and Hocenski, Ž. (2016) 'Cloud computing security issues and challenges', Research Gate.

[14] Schouten, E. (2014) Cloud computing defined: Characteristics &amp; service levels - Cloud computing news. Available at: https://www.ibm.com/blogs/cloud-computing/2014/01/31/cloud-computing-defined-characteristics-service-levels/ (Accessed: 10 April 2018).

[15] Sen, J. (no date) 'Security and Privacy Issues Cloud Computing'. Available at: https://pdfs.semanticscholar.org/4dc3/70d253020947a8e66b701e12dd0233161229.pdf (Accessed: 11 April 2018).

[16] Siddaway, D. A. (no date) 'WHAT IS A SYSTEMATIC LITERATURE REVIEW AND HOW DO I DO ONE?'

[17] Suri, J. M. and Nath, T. B. K. (no date) 'Security and Privacy in Cloud Computing'. Available at: http://tec.gov.in/pdf/Studypaper/Paper-1-security and Privacy.pdf (Accessed: 12 April 2018).

[18] TagElsir Ahmed Osman, T., babiker, A. A. and Mustafa, N. (2015) 'External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view', IOSR Journal of Computer Engineering Ver. V, 17(2), pp. 2278–661. doi: 10.9790/0661-17259396.

[19] Takabi, H., Joshi, J. B. D. and Ahn, G.-J. (2010) 'Security and Privacy Challenges in Cloud Computing Environments', IEEE Security & Privacy Magazine, 8(6), pp. 24–31. doi: 10.1109/MSP.2010.186.