International Journal of Engineering & Technology, *7 (4.19) (2018) 127-133*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Threats and Existing Solutions on Cloud Computing

Faisal Shahzad[1*], Roshidi Din[2], Osman Ghazali[3]

[1]Department of Computer Science & IT, TheIslamia University of Bahawalpur, Punjab, Pakistan
[2, 3]School of Computing, Universiti Utara Malaysia, UUM, Kedah, Malaysia
**Corresponding Author E-mail: [1]faisalsd@gmail.com*

Abstract

Cloud computing as the greatest evolution of distributed computing, gets benefitted from the technology advancement due to its data versatility and economies of scale. Cloud computing aims to offer flexible services that can minimize the customer's need for investing in new hardware and software. However, the rapid extension of cloud computing raises some concerns regarding security and privacy of data that appears to be an inhibitor in the adoption of cloud services. It is, therefore, necessary to address these issues and their existing solutions. For this purpose, the present study is engrossed in the security threats to data that have been listed as the top threats in the previous years. Mainly, this study provides a review of top threats to cloud security and the solutions based on different models, frameworks, and algorithms to ensure data security in a cloud environment. The significance of this paper is twofold as it provides an overview of security threats as well as it explores the existing solutions to the problem in data security in cloud computing. The outcomes of this study presented that there is still a need for accurate mechanism or technique that can minimize the security threats faced in cloud computing.

Keywords: *Cloud computing, Data breach, Data privacy, Data confidentiality, Cloud security,*

1. Introduction

Cloud computing is a new computing paradigm which is advancing rapidly as the new model for service delivery of Information Technology (IT). It is a computing style that provides a scalable and virtualized resources over the internet where users are not having any expertise in technology infrastructure that can support them which in turn enables the on-demand provisioning of computational and storage resources. Cloud computing has been defined variably by voluminous studies, however, none of the definition found worldwide recognition. Amongst the several definitions, the definition presented by the National Institute of Standards and Technology (NIST) covers almost all important characteristics of cloud computing and is recognized broadly.

The NIST states that “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction”[1].

In accordance with the definition and characteristics presented by NIST, cloud computing has five main characteristics named as on-demand self-services, resource pooling, broad network access, rapid elasticity and measured service[2]. Moreover, considering the architecture, NIST stated that cloud consists of three service models named as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The cloud architecture as a whole with the complexity of cloud security domains and aspects is depicted in Figure 1.

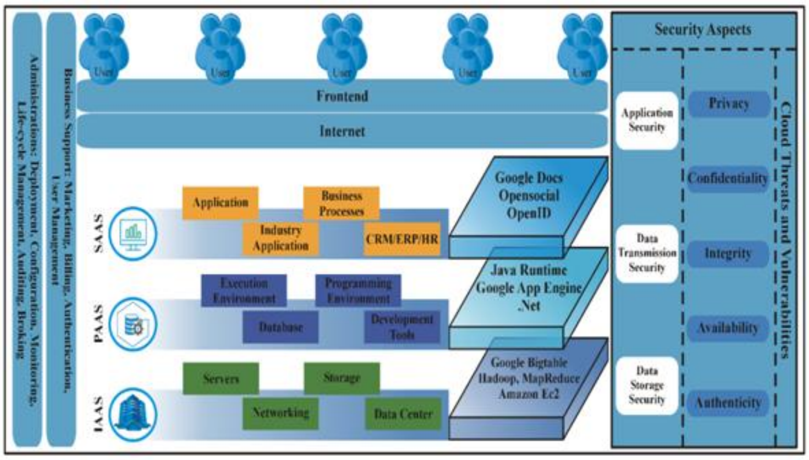
Administrations: Deployment, Configuration, Monitoring, Life-cycle Management, Auditing, Broking
Business Support: Marketing, Billing, Authentication, User Management
User
User
User
User
User
Frontend
Internet
SAAS
Application
Business Processes
Industry Application
CRM/ERP/HR
Google Docs Opensocial OpenID
PAAS
Execution Environment
Programming Environment
Database
Development Tools
Java Runtime Google App Engine .Net
IAAS
Servers
Storage
Networking
Data Center
Google Bigtable Hadoop, MapReduce Amazon Ec2
Security Aspects
Application Security
Data Transmission Security
Data Storage Security
Privacy
Confidentiality
Integrity
Availability
Authenticity
Cloud Threats and Vulnerabilities

Fig. 1: Cloud Architecture environment and security domains (based on [3]–[5])

Figure 1. presents the broad architecture of a cloud computing paradigm. Building upon hardware and software facilities that are supported by the data center, the services of the cloud may be offered from the bottom to top layer where each layer represents one service delivery model. These three layers as stated above represent different delivery models i.e. SaaS, PaaS, and IaaS. These three service models are the core of cloud with each layer exhibiting certain characteristics sorted upwardly. Additionally, some noteworthy challenges to the security of data such as security of data storage, security during transmission of data and application security are also mentioned with cloud threats and vulnerabilities occurring in each delivery model[6].

Additionally, this figure is complemented with IT-related infrastructure supporting operations of all models. This figure shows the intermediated layer of internet lying between clouds and customers. On another hand, specific business and administration strategies are employed in order to manage cloud in a better way and to fulfill the needs of customers[3]–[5].

Given the appealing characteristics and architecture of the cloud computing, it has been found that cloud is becoming a widespread business model for both academia and industry. However, these beneficial features of cloud computing result in some serious cloud-specific security concerns[7], [8]. These security concerns are appearing to be the dominant barrier to expansion and adoption of the cloud computing and have been addressed widely. Several researchers have provided different solutions to assure security in cloud computing, however, this issue of data security still prevails. Thus, keeping in view the security of cloud as a major concern, the present paper aims to provide a survey on the topic of cloud security in particular. This paper includes the studies from both academia and industry and explores the strengths and limitations of the existing literature.

2. Related Work

Currently, the security state of cloud computing is discussed widely in both academia and industry. As mentioned earlier, the security issues in cloud computing are increasing parallel to the growth of cloud computing that leads to the inhibition of organizations to shift to the cloud environment. In the last decade, these security concerns have been the major focus of researchers and industries as threats to the cloud environment are obstructing the transition of data of the big companies to the cloud environment.

Considering this, voluminous studies have been published that are described in the proceeding section. In the current era, the prominent threats to the cloud computing has been reported by several researchers that includes the work by Behl[9] who in 2011, stated major security threats; where Silva[10]in 2013 provided detailed taxonomy of these threats by considering 661 publications that have previously addressed the security threats to the cloud computing. Later in 2015, Irfan[11] also reported the threats that have been widely discussed previously.

Moreover, Eken[12] has also identified major threats to security in cloud computing faced by companies and industries whereas Kulkarni[13], focused on service models SaaS, PaaS and IaaS and ways to secure data in the cloud for making this technology better. On other hand, benefits and issues related to data security in the cloud are discussed by Sugumaran et al. [14]. Additionally, Ghorbel[15] also did a survey on breach of privacy in a cloud environment and discussed the research challenges as well as Bhadauria[16] conducted a survey on security issues by discussing associated mitigation techniques.

In addition to that, Cloud Security Alliance (CSA) has also published different reports in 2010 [14], 2013 [16] and 2016 [17] that targeted the top threats to security in cloud computing and has been accepted widely by the cloud users. Therefore, the current paper explores the literature that deals with security threats listed in the guide entitled “The Treacherous 12 - Cloud Computing Top Threats” on February 29, 2016, from Cloud Security Alliance (CSA).

3. Overview of Cloud Security Threats

With the speedy progression of cloud technology, several new services are also emerging that appears to be a great news for enterprises who want to achieve goals quickly and easily, on contrary, security is making them move from their target. Faulty cloud implementations and security issues may prove difficult for industries to shift to the cloud environment. Therefore, security of data in the cloud is a top priority whether the cloud is in on-premises, off-premises or a hybrid. For this purpose, the CSA reports of the year 2010, 2013 and 2016 provided an overview of security threats to cloud computing where data breach was found to be among the top security threats. The purpose of these reports was to provide an updated understanding of cloud security aspects to the organizations to develop strategies of risk management for cloud adoption. These reports reflect the consensus of all security experts regarding the cloud security issues.

In 2010, CSA published a report, “Top Threats to Cloud Computing, Version 1” and discussed the best practices in cloud computing and identified the top threats in cloud computing. The report spread the awareness in cloud domain and described the threats in detail with their corrective measures[17].

Subsequently, in 2011, the CSA published its third version titled as “Security Guidance for Critical Areas of Focus in Cloud Computing” and identified fourteen “domains of concern” in cloud networks. Another report named “Security as a Service Implementation Guidance” was also published. In first report, each threat described in version 1 was linked to the domain of cloud computing architectural framework that was reported in the later report[16]–[18]. These both documents rapidly became the industry-standards catalog of best practices to secure cloud computing. These documents addressed the best practices within the fourteen domains of CSA Guidance and ten categories of service associated with the SaaS Implementation Guidance series. This guidance[19] is later incorporated into the cloud strategies by various organizations, businesses, and government departments. This report provided an updated guide that helps the cloud consumers and providers to make potential decisions about risk management within a cloud.

Later, in 2013, the CSA published an advanced form of these works named as “The Notorious Nine Cloud Computing Top Threats” [19]. This report provided an updated list of top threats that increases in comparison to the list of 2010. Further, in 2016,“The Treacherous 12 - Cloud Computing Top Threats in 2016” [20]appears as an important report in CSA research network. Besides numerous security concerns in the cloud, this report listed 12 threats specifically related to the shared, on-demand characteristic of cloud computing [21]. In order to identify these top 12 threats, a survey of industry experts was conducted by CSA to obtain an opinion from professionals about major security issues in cloud domain. The groups working on Top Threats along with their expertise used the survey results to compile the final report of 2016.

Besides the identification and description of security threats, a threat analysis was also conducted with the STRIDE Threat Model [22] that was developed by Microsoft to assess information about security threats. Basically, STRIDE is an acronym defining a system of threat classification and stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. The particular security concerns in that paper were evaluated to determine whether they reside in any of the following threat categories.

In summary, these 12 major security threats along with the CSA security guidance reference domains, cloud service delivery models and the STRIDE threat model analysis are elaborated in the following Table 1.

Table 1: The Treacherous 12, domains and service delivery models with STRIDE threat model

Threat#	Threat Name	CSA Security Guidance Reference Domain (s)#	Cloud Service Delivery Model Applicability			STIDE Threat Model Analysis					
			IAAS	PAAS	SAAS	Spoofin g Identit	Tampe ring With	Repudi ation	Inform ation Disclos	Denial of Service	Elevati on of Privileg
1	Data Breaches	D5,D10,D1,D11,D12,D13	✓	✓	✓	×	×	×	✓	×	×
2	Weak Identity, Credential and Access Management	D11,D12	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Insecure Interfaces and APIs	D5,D6,D9,D10,D11,D12	✓	✓	✓	×	✓	✓	✓	×	✓
4	System and Application Vulnerabilities	D1,D2,D7,D8,D10,D13	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	Account Hijacking	D2,D5,D7,D9,D11,D12	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Malicious Insiders	D2,D5,D11,D12	✓	✓	✓	✓	✓	×	✓	×	×
7	Advanced Persistent Threats (APTs)	D1,D2,D7,D8,D10,D13	✓	✓	✓	×	×	×	✓	×	✓
8	Data loss	D5,D10,D12,D13	✓	✓	✓	×	×	✓	×	✓	×
9	Insufficient Due Diligence	D1,D2,D3,D4,D5,D6,D7, D8,D9,D10,D11,D12,D13,D14	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Abuse and Nefarious Use of Cloud Services	D3,D7,D9	✓	✓	✓	×	×	×	×	✓	×
11	Denial of Service	D8,D9,D10,D13,D14	✓	✓	✓	×	×	×	×	✓	×
12	Shared Technology Issues	D1,D5,D11,D12,D13	✓	✓	✓	×	×	×	✓	×	✓

Note: A check mark (√) means the threat affects the underlying models and the cross (X) means otherwise.

Table 1.summarizes the research works that overviewed the topic of cloud security. Both the Cloud security alliance (CSA) and STRIDE threat model are presented to evaluate information about security threats. It presents 12 security threats that have been mentioned by CSA (2016) report as well as identifies the security domains involved in each threat. It also presents the top threats mentioned by the CSA, the domains in which they are included, the service delivery models and stride threat model they affect. A threat analysis was also conducted with the STRIDE Threat Model showing that threat to security is at all deployment layers.

4. Existing Studies on Security Threats

Parallel to the wide landscape of security in the cloud, the concerns about the security are several and require to be addressed on the vast scale considering all of the threats to security. Though number of studies has been presented whereas little attention was given to the role of clouds in IT and cybersecurity. As stated earlier, this study purports to examine the existing researches that have been conducted on the security of data in cloud computing. Therefore, it is pertinent to study the prevailing work for the security of data so that the limitations in the previous work could be explored.

Existing literature on cloud computing and its security aspects has presented a number of studies that have proposed different models, frameworks, and algorithms assuring the data security in the cloud environment. The analysis of some of the recent studies conducted on the topic of data security and solutions to prevent its breach are presented in following Table 2. Along with the strengths and weaknesses of each of them.

Table 2: Existing Studies on Security Threats

Researcher	Topic Focused	Strengths	Limitations
Jansen, 2011 [23]	Cloud security and privacy issue on the public cloud.	Theoretical research provides the existing security issues	No framework /model is proposed to address the identified issue.
Behl, 2011 [9]	Emerging security concerns in cloud computing.	Security challenges and their appropriate solutions are provided.	No model or framework of solutions is provided.
Joeng-Min et al. 2011 [24]	Attribute-based Proxy Re-Encryption for preserving Data Confidentiality	Ensures security against collusion attack	Requires much effort to handle and communicate and do not ensure the integrity
Jaatun et al. 2011 [25]	A farewell to trust: An approach to confidentiality control in the cloud	Introduced RAIN approach to categorize the data and ensure security	No experimentation and practical implementation is validated
Prasad et al. 2011 [26]	3D security in cloud computing	Ensures data availability and flexibility	No implementation detail No integrity check
Feng 2012 [27]	Applying Agents to the Data Security	Present and introduces agents to data security	No detailed verification
Kulkarni et al. 2012 [13]	Cloud security aspects by emphasizing on data privacy protection.	Recommends various encryption and decryption techniques for secure transmission of data.	Only theoretical issues related to encryption and decryption techniques are discussed without a proposed model.
Kumar et al. 2012 [28]	The methodology of cloud storage by using elliptic curve cryptography encryption.	Data is secured until it is encrypted only authenticated user can access the data.	Provided methodology focusing only on encrypted data and simulation or implementation results are not provided.
Nashaat. 2012 [29]	A model to secure data while stored in Cloud	Enhance security of stored data by using scheme names "Defense in Depth".	Reliability of retrieved data is not guaranteed
Chandramohan et al. 2013 [30]	Privacy-preserving algorithm to preserves the confidentiality of stored data using mitigation methodology.	Preserving privacy and scrutinizing issue.	Third party authentication privacy framework is required.
Eken, 2013	Major security threats in the cloud	Data security solution provided to cloud	On the basis of discussion, no innovative

[12]	and the associated risk.	providers and enterprises	model or framework is proposed.
Ikechukwu et al. 2013 [31]	Building Trust and Confidentiality by proposing an information-centric approach	Solves problems of data security by building trust	No implementation
Chandramohan et al. 2013 [32]	Onion and garlic encryption framework for prevention of data loss while storage in the cloud.	Information is secured by multiple encryptions of onion and garlic privacy preserving layered approach.	Theoretical framework with no implementation details.
Arockiam et al. 2014 [33]	Obfuscrypt in combination with encryption deals with confidentiality of data storage	Offers better security and overtakes existing techniques that use obfuscation or encryption alone	Does not involve any integrity verification mechanism.
Doe et al.2014 [34]	Prevents data breach by providing user authentication through a one-time password system	To protect privacy and confidentiality of data and detect and prevent possible risks.	Data breach prevention on one platform only using Google App
Gawande et al. 2014 [35]	Analysis of data confidentiality techniques in cloud computing	Fewer cloud providers are required to store fragmentation and reduce computations overhead	Not efficient outsourced database and computation cost Does not guarantee data integrity
Sugumaran et al. 2014 [14]	Architecture to store encrypted data on the cloud using block cipher symmetric cryptography algorithm.	Used symmetric cryptography to overcome the security issues efficiently.	No implementation procedure.
Irfan et al. 2015 [11]	QR Code with 3DES Algorithm to efficiently store data.	Completely secure for unauthorized access. Even the user gets data in an encrypted form that needed to be decrypted on user site.	Minimizing performance of the algorithm and increases computational complexity.
Chang et al. 2015 [36]	To achieve security of data security with cloud computing adoption framework	Three-layer Framework to protect data security i.e. firewall and access control, identity management and intrusion prevention and convergent encryption	The framework is in its early developmental stage and requires further simulations to verify the performance.
Algarni et al. 2016 [37]	A consolidated approach for estimation of data security breach costs	Open quantitative data of data breach and cost	Computation of probability factor needs to be explored in detail
Mahalakshmi et al 2016 [38]	Security-as-a-service for files in cloud computing- A novel application model	A new security-as-a-service based application model is proposed and works well against cryptanalysis	Key size is limited and limited parameters are verified
Tchernykh et al. 2016 [39]	Uncertainty in cloud computing with risks of confidentiality, integrity, and availability	Address methods to mitigate the risks of confidentiality, integrity, and availability linked to the loss of information	Scheme handles only a limited risk related to CIA model.
Huson et al. 2016 [40]	Increased regulation result in a reduction in information compromises.	Examine the effectiveness of regulation to determine whether increased regulation would result in a reduction in information compromises.	Difficult to reduce data breaches with different regulations
Verginadis 2017 [41]	PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services	Proposed PasSword- a noble holistic framework	Not fully functional solution
Mishra 2018 [42]	Secure Framework for Data Security in Cloud Computing	Proposed model for ensuring security and integrity in cloud	The proposed model requires further simulations to verify the performance.

In Table 2, Jansen [23][20] highlighted the benefits of cloud computing along with the basic security issues. This study has provided an insight to the end users about the security whereas it does not propose any framework or tool that can address the identified security issues. Moreover, the study of Behl [6] focused on cloud-related security issues and existing approaches to securing applications by removing the drawbacks. Although, this study discussed several critical security issues and provided the appropriate solutions, however, it does not propose any specific model or algorithm to solve the issue. In addition, Joeng-Min et al [24] performed proxy re-encryption for data confidentiality to ensure security against collusion attack. However, it requires much effort to communicate and does not handle integrity.

Furthermore, Jaatun[25], for the categorization of data introduced RAIN approach to ensure security. This study did not validate the experimentation and practical implementation. Likewise, Prasad et al.[26] [23] proposed 3D security in cloud computing that ensures availability and flexibility and did not provide any implementation detail and there is no check on integrity. Feng[27] applied agents to data security wherein, no detailed verification is provided. Additionally, Kulkarni et al. [10] depicted that data privacy protection is considered as one of the major challenges to the cloud. This work recommended that cloud computing should be established on different encryption and decryption techniques for secure transmission of data, however, it does not provide any methodology or model to avoid all threats.

Kumar et al.[28] provided a method that ensures the security and data privacy from the cloud provider. Elliptic Curve Cryptography (ECC) was used to protect the user data from an intruder and also from the cloud data storage provider. Preserving and accessing data is more secure through this methodology and it can also solve the group sharing problem of data in the shared data section. Moreover, Nashaat et al.[29] [26] proposed a model for enhancing data security by using “defense in depth” scheme whereas, it does not guarantee the reliability of the retrieved data. Later, Chandramohan et al.[30] developed the mitigation methodology for preserving the privacy by developing a privacy-preserving algorithm. This algorithmic approach helps in mitigating the privacy preservation breeze and scrutinizing this issue. This research work is limited to one dimension which is algorithm based user identification and testing results of an algorithm were also not provided.

Furthermore, Eken[12]also identified major security threats to cloud computing. This work provided a security threat solution without any new innovation related to security of cloud computing. This work could have presented any new methodology or mechanism for preserving the data in the cloud. Moreover, Ikechukwu et al.[31] presented an information-centric approach that helps in solving problems in distributed storage by building trust, however, no implementation detail is presented. Moreover, a layered framework by Chandramohan et al.[32]was introduced for preserving the secrecy of data and digital loss. Techniques used for data encryption were Onion and Garlic Privacy Preserving Approach (OGPPA), Onion Privacy Preserving Approach (OPPA) and Garlic Privacy Preserving Approach (GPPA). However, three-factor encryption could be the focus of this research for preventing privacy breach and it could also mention the results of implementation and testing.

Later, Arockiam et al. [33] used Obfuscrypt along with encryption that could better deal with the cloud security and outperforms existing techniques that use obfuscation or encryption alone whereas it does not provide any integrity verification mechanism. In addition, Doe and Suganyain [34]proposed a framework that prevents data breaching threat. It provided user authentication through one-time password system to prevent risk and ensure secure key management by elliptic curve cryptography with a random number along with integrity with the MD5 mechanism. This study could have implemented preventive measures to reduce other threats, as well as deployment can be done on different cloud platforms to ensure its usage across platforms. In [35], Gawande focuses on the secure outsourcing of data by using Fragmentation and high-Performance Anonymization Engine techniques and applying only minimal encryption to prevent data exposure. This study lacks in providing reduced communication and computation cost and the optimization of query processing time can also be improved.

On contrary, Sugumaran et al. in [14]proposed an architecture of "block cipher cryptographictechnique" to store data on the cloud. The proposed architecture can overcome the issues of security by implementing cloud as an efficient technology for storing consumer's data speedily however, the implementation detail of the architecture was missing that would be helpful in verification of data. On another hand, Irfan et al. [11]proposed a methodology for solving the security issues faced by cloud computing. The proposed solution is the merger of "QR Codes" and "Triple Data Encryption Standards Algorithm". The Key will be unique and data will not be easily accessed by any intruder, yet there are chances that computational complexity will lessen the performance of algorithm whereas QR code used in this proposed model is not widely used in the cloud environment. In the same year, Chang et al.[36]proposed three-layered framework to secure data by controlling firewall and access, by the management of identity and intrusion prevention and convergent encryption. However, this framework requires more efficiency and development.

In 2016, Algarni et al. [37] provided a consolidated approach for estimating data breaches and studied quantitative data of data breach and cost. Whereas, computation probability factor needs to be explored further. Additionally, Mahalakshmi et al. [38]proposed a novel application model i.e. security-as-a-service for files in cloud computing that works well against cryptanalysis. However, the key size is limited and limited parameters were verified. Furthermore, Tchnernykh[39]discussed the role of uncertainty in the resource especially in presence of risks to integrity, confidentiality, and availability. This paper addressed methods to mitigate the risks related to loss of information, data leakage and denial of service.

Additionally, Huson et al.[40]examined the regulatory environment as it is relevant to compromise of personally identifiable information. Compromises happen regardless of 2639 approaches. Though compliance may be an issue in some of the more spectacular beaches, there are operational and economic reasons to allow even noncompliant entities to continue operating. Even with evidence that few regulations are able to reduce loss due to data compromise, there is no indication that fewer compromises are the result of an increase in regulations. Moreover, Verginadis[41]highlighted security challenges while shifting to cloud and proposed a novel holistic framework named PaaSword that seeks to deal with these challenges. In particular, it involves a context-aware security model, policy enforcement mechanism and encryption. However, the solution was not fully functional. Recently, Mishra [42]proposed model for securing data and its integrity in cloud computing, however, this model requires further simulation to verify the performance. Hence, researchers have considered both physical and logical security issues across all service and delivery models and provided solutions to secure data in cloud computing. However, the techniques lack in some critical issues such as low cost, security and time and implementation of complexity related issues.

5. Discussion

The present paper presented an overview of security threats to cloud computing that has been pointed out by various researchers working in the field of cloud security. A number of organizations are focusing on improving the security issues by developing solutions and standards to solve this problem. In the past couple of years, interesting research has appeared concerning the security of the cloud. The researchers collected data from the customers and report findings of the trends and threats to security in a cloud environment. Other studies discussing IT include cloud computing and interesting facts about it as such studies aim to share intelligence with other organizations and communities doing research on the security of cloud environment.

The 2013 report of CSA highlighted that developers and IT departments bypass the organizational security requirements by rolling out their own self-service shadow IT projects. Whereas, the top threats that have been highlighted in the 2016 report has provided the consequences of shifting to cloud technology by managerial ranks which became a boardroom issue rather than an IT issue. It was found that executive strategies may be aligned with the adoption of cloud in order to maximize the shareholder value.

Though the existing techniques and mechanisms can fulfill many security challenges theoretically, still there are many security concerns in a cloud environment. Initially, the issue of lack of user control in the cloud needs to be resolved. In fact, studies have addressed this issue by supportingpolicy enforcement of data owner and auditing for data security assurance. Yet, unless the visibility and transparency of data are not protected while processing data, there are chances of vulnerability that appears to be a threat to data. Hence, a number of studies are still required to retain control for data owner while data is processed and stored in the cloud.

Therefore, it can be concluded that protection of security needs to be the focus of prospective studies and more solutions are required to address this issue of security in a cloud environment. The proposed solutions should consider all aspects of security which enables complete security protection. Nevertheless, it is difficult since security is not adopted during designing of the cloud environment.

6. Future Directions

Considering the aforementioned studies, a deeper insight of techniques to secure data is obtained which provides the information that every proposed technique poses a specific challenge which prevents them from being the best solution. Some of the challenges observed are; securing data without burdening the cloud server, developing model that address all data security issues, using schemes that do not cause a delay in the network and supporting all changes. Prospective researchers should consider all these challenges and try to devise a technique that could rule out all insecurities to data in the cloud environment.

In addition, developers should take into account the security issues and devise application software that should both scale down and scale up rapidly. It is because potential users would not rely completely on this technology unless an effective security model is developed that caters all security issues arising in a cloud environment. Moreover, in the cloud, each element should be examined at micro and macro level with the development and deployment of an integrated solution in order to attract the potential consumers and to reduce security threat.

Furthermore, at a regular basis, an auditing should be done to protect cloud against external threats. Additionally, human errors should be reduced and it should be ensured by cloud providers that all SLA's are met in order to have a smooth functioning. Thus, protection of data in the cloud is complex and requires the intervention of all potential researchers who can help in securing data in cloud computing.

7. Conclusion

Cloud computing has undoubtedly transformed the world of computing by providing multiple benefits. However, some threats to security in cloud arise parallel to the advantages of this technology. To address these security issues, the present paper presented an overview of the existing threats to a cloud environment. Representative security threats were identified and discussed by presenting the report by CSA and using STRIDE threat model. Additionally, different approaches in existing studies were highlighted that are proposed to secure data in cloud computing. It has been analyzed that there are several techniques that deals with the issues of security of data, however, none of them have introduced any technique that can completely ensure the security of data at all levels of service models.

Therefore, keeping in view the panorama, it has been observed that besides various advantages of cloud, there are number of practical problems that should be solved. These problems are related to the security and privacy of data in a cloud environment. To address this issue, an appropriate technique should be devised that can cater all the security problems that appear to be an inhibitor in the adoption of cloud. Unless an appropriate strategy is not implemented, the users will not be able to fully enjoy the benefits of cloud computing and its environment will remain cloudy.

Conclusively, it would not be wrong to say that cloud environment entails a broad range of security threats that inhibit the consumers to shift to this technology. Therefore, by considering above stated discussion, it is deemed necessary to continue the research on dealing with the security issues in order to achieve more secure, trustworthy and reliable cloud environment.

Acknowledgement

This research is fully supported by University Research Grant from Sultan Idris Education University under the grant number of 2018-0134-109-01.

References

[1] P. M. Mell and T. Grance, “The NIST definition of cloud computing,” Gaithersburg, MD, 2011.

[2] M. Armbrust et al., “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, p. 50, Apr. 2010.

[3] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[4] Z. Xiao and Y. Xiao, “Security and Privacy in Cloud Computing,” IEEE Commun. Surv. Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[5] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, “Security issues in cloud environments: a survey,” Int. J. Inf. Secur., vol. 13, no. 2, pp. 113–170, Apr. 2014.

[6] A. Sarwar and M. N. Khan, “A Review of Trust Aspects in Cloud Computing Security,” Int. J. Cloud Comput. Serv. Sci. , vol. 2, no. 2, pp. 116–122, 2013.

[7] A. Kumar, “World of Cloud Computing &amp; Security,” Int. J. Cloud Comput. Serv. Sci. , vol. 1, no. 2, pp. 53–58, 2012.

[8] D. Gaurav Pal, R. Krishna, P. Srivastava, S. Kumar, M. Bag, and V. Singh, “A Novel Open Security Framework for Cloud Computing,” Int. J. Cloud Comput. Serv. Sci., vol. 1, no. 2, pp. 42–52, 2012.

[9] A. Behl, “Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation,” in 2011 World Congress on Information and Communication Technologies, 2011, pp. 217–222.

[10] C. M. Revoredo da Silva, J. L. Costa da Silva, R. B. Rodrigues, G. M. Medeiros Campos, L. Marques do Nascimento, and V. Cardoso Garcia, “Security Threats in Cloud Computing Models: Domains and Proposals,” in 2013 IEEE Sixth International Conference on Cloud Computing, 2013, pp. 383–389.

[11] M. Irfan, M. Usman, Y. Zhuang, and S. Fong, “A Critical Review of Security Threats in Cloud Computing,” in 2015 3rd International Symposium on Computational and Business Intelligence (ISCBI), 2015, pp. 105–111.

[12] H. Eken, “Security threats and solutions in cloud computing,” in World Congress on Internet Security (WorldCIS-2013), 2013, pp. 139–143.

[13] G. Kulkarni, J. Gambhir, T. Patil, and A. Dongare, “A security aspects in cloud computing,” in 2012 IEEE International Conference on Computer Science and Automation Engineering, 2012, pp. 547–550.

[14] M. Sugumaran, B. B. Murugan, and D. Kamalraj, “An Architecture for Data Security in Cloud Computing,” in 2014 World Congress on Computing and Communication Technologies, 2014, pp. 252–255.

[15] A. Ghorbel, M. Ghorbel, and M. Jmaiel, “Privacy in cloud computing environments: a survey and research challenges,” J. Supercomput., vol. 73, no. 6, pp. 2763–2800, Jun. 2017.

[16] R. Bhadauria and S. Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques,” Cryptogr. Secur., Apr. 2012.

[17] Cloud Security Alliance, “Top Threats to Cloud Computing V1.0,” Cloud Security Alliance., 2010. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[18] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v3.0,” 2011.

[19] Cloud Security Alliance, “The Notorious Nine. Cloud Computing Top Threats in 2013,” Security, 2013. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats.%5Cnhttp://www.cloudsecurityalliance.org.

[20] Cloud Security Alliance, “The Treacherous 12 Cloud Computing Top Threats in 2016,” Security, no. February, pp. 1–34, 2016.

[21] R. Barona and E. A. M. Anita, “A survey on data breach challenges in cloud computing security: Issues and threats,” in 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT), 2017, pp. 1–8.

[22] “The STRIDE Threat Model,” 2011. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx. [Accessed: 18-May-2018].

[23] W. A. Jansen and W. A., “Cloud Hooks: Security and Privacy Issues in Cloud Computing,” in 2011 44th Hawaii International Conference on System Sciences, 2011, pp. 1–10.

[24] D. Jeong-Min, S. You-Jin, and P. Namje, “Attribute Based Proxy Re-encryption for Data Confidentiality in Cloud Computing Environments,” in 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, 2011, pp. 248–251.

[25] M. G. Jaatun, A. A. Nyre, S. Alapnes, and G. Zhao, “A farewell to trust: An approach to confidentiality control in the Cloud,” in 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011, pp. 1–5.

[26] P. Prasad, B. Ojha, R. R. Shahi, R. Lal, A. Vaish, and U. Goel, “3 dimensional security in cloud computing,” in 2011 3rd International Conference on Computer Research and Development, 2011, pp. 198–201.

[27] Feng-qing Zhang and Dian-Yuan Han, “Applying agents to the data security in cloud computing,” in 2012 International Conference on Computer Science and Information Processing (CSIP), 2012, pp. 1126–1128.

[28] A. Kumar, B. G. Lee, H. Lee, and A. Kumari, “Secure storage and access of data in cloud computing,” in 2012 International Conference on ICT Convergence (ICTC), 2012, pp. 336–339.

[29] D. N. El-khameesy, D. N. El-khameesy, and H. A. Rahman, “A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems,” J. Emerg. TRENDS Comput. Inf. Sci. Vol. 3, ISSUE 6, pp. 970--974, 2012.

[30] D. Chandramohan, T. Vengattaraman, D. Rajaguru, R. Baskaran, and P. Dhavachelvan, “A privacy breach preventing and mitigation

methodology for cloud service data storage," in 2013 3rd IEEE International Advance Computing Conference (IACC), 2013, pp. 83–88.

[31] I. Uegebe and U. Omenka, Building trust and confidentiality in cloud computing distributed data storage, vol. 6, no. 1. Olliverson Industrial Publishing House, 2013.

[32] D. Chandramohan, T. Vengattaraman, D. Rajaguru, R. Baskaran, and P. Dhavachelvan, "A novel framework to prevent privacy breach in cloud data storage area service," in 2013 International Conference on Green High Performance Computing (ICGHPC), 2013, pp. 1–4.

[33] L. Arockiam, S. Monikandan, and P. D. Sheba K Malarchelvi, "Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage," Int. J. Comput. Appl., vol. 88, no. 1, pp. 17–21, Feb. 2014.

[34] N. P. Doe and Suganya V., "Secure service to prevent data breaches in cloud," in 2014 International Conference on Computer Communication and Informatics, 2014, pp. 1–6.

[35] M. R. Gawande and A. S. Kapse, "Analysis of Data Confidentiality Techniques in Cloud Computing," Int. J. Comput. Sci. Mob. Comput., vol. 3, no. 3, pp. 169–175, 2014.

[36] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," IEEE Trans. Serv. Comput., vol. 9, no. 1, pp. 138–151, Jan. 2016.

[37] A. M. Algarni and Y. K. Malaiya, "A consolidated approach for estimation of data security breach costs," in 2016 2nd International Conference on Information Management (ICIM), 2016, pp. 26–39.

[38] J. Mahalakshmi and K. Kuppusamy, "'Security-as-a-Service' for files in cloud computing — A novel application model," in 2016 10th International Conference on Intelligent Systems and Control (ISCO), 2016, pp. 1–5.

[39] A. Tchernykh, U. Schwiegelsohn, E. Talbi, and M. Babenko, "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," J. Comput. Sci., Nov. 2016.

[40] M. L. Huson and B. Hewitt, "Would Increased Regulation Reduce the Number of Information Breaches?," in 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 2633–2641.

[41] Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hübsch, and I. Paraskakis, "PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services," J. Grid Comput., vol. 15, no. 2, pp. 219–234, Jun. 2017.

[42] N. Mishra, T. K. Sharma, V. Sharma, and V. Vimal, "Secure Framework for Data Security in Cloud Computing," Springer, Singapore, 2018, pp. 61–71.