INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Privacy and trust in cloud computing

Faisal Alghayadh
falghayadh@oakland.edu
Oakland University, Rochester, Michigan

Yasamin Alagrash
yhalagrash@oakland.edu
Oakland University, Rochester, Michigan

Debatosh Debnath
debnath@oakland.edu
Oakland University, Rochester, Michigan

ABSTRACT

This paper focuses on analyzing security and privacy problems facing cloud computing. The major issue discussed in the research that of losing control of data by both the cloud service providers (CSPs) and cloud service users (CSOs). Cloud computing offers organizations an innovative business model to adopt IT services without having to incur massive investment costs. A general analysis of the cloud is provided including its various forms. The growth and development of cloud computing technology are hampered by the fears of losing control of sensitive data by corporations and individuals. Solutions regarding this problem are discussed, and an intensive elucidation of the optimal one is included.

Keywords— *Privacy, Security, Cloud computing*

1. INTRODUCTION

Over the years, the world has continued to become more competitive thereby leading to improved innovations and creativity. Technology has redefined peoples' way of thinking over and above operations. The Internet and the World Wide Web are among the notable innovations that have introduced significant impetus to the technological world [8]. Albeit technology reinvigorating the world with substantial gains, some numerous challenges have arisen leading to the development of cloud technology which is intended to address the storage issue. Though cloud computing has been able to solve the storage problem considerably, experts have realized some security hiccups related to it [5]. On that background, this paper will focus and provide detailed information regarding losing control of data as a major problem associated with cloud computing.

Cloud computing exists in three distinct forms namely: hybrid, private, and public clouds. A public cloud refers to one where the cloud providers utilize the internet for purposes of coming up with resources including storage and applications [9]. A private cloud refers to the data center architectures solely owned by a company [9]. The cloud provider provides provisioning, scalability, flexibility, monitoring, and automation. A private cloud targets to gain the cloud architecture benefits devoid of giving up the maintenance control of the data center. On the other hand, the hybrid approach entails corporations relying on the public cloud and at the same time maintaining control of a private control managed data center internally [1][9].

The adoption of cloud computing by firms and individuals is interpreted as the sharing of data with a CSP [10]. The cloud model results in loss of data control by both the CSUs and CSPs. Cloud security experts have expressed concerns about storing data that is highly confidential in the infrastructure. Notably, loss of control refers to a situation whereby cloud user's control over their data gets diminished during the moving of data to remote cloud servers from their local servers [11]. Nonetheless, cloud computing is believed to be attack-proof from hackers hence promoting its preference in hosting such data.

1.1 Research problem

The cloud providers are seemingly not aware of the confidentiality and security requirements regarding data hosted on their infrastructure. On the other hand, the user is not in a position to control either the system security apparatus as well as the other services sharing the same resources [1]. This opens doors to a number of security and privacy concerns.

By description the Cloud Service threat profile. Given the right circumstance, an attacker can translate these threats to exploits and compromise the corresponding infrastructure or the application implemented as a Cloud Services. The rest of the paper is organized as follows: - the next section identifies loss of control. Section III reviews the current solutions. Section IV presents a scenario of secure cloud computing techniques. Finally, section V discusses the conclusion and new research directions.

2. LOSS OF CONTROL

Loss of data control results in problematic situations revolving around data integrity and data confidentiality. Based on a research by International Data Corporation (IDC), a majority of the CIOs have raised serious concerns regarding loss of control as a major security problem associated with cloud computing [1]. Upon giving control of data to the hosting CSP, the information becomes more susceptible to suffering from damage especially during transitions from one provider to another [8].

A majority of the cloud service providers present the user with terms and conditions that are unfavorable in enhancing control of the stored data. The social media sector is an excellent example of firms that make profits by leveraging the private

information of an individual [8]. Enterprises that are dependent on cloud computing are more likely to obtain information from the cloud without the owner's consent. This is a risk facing a majority of the corporations particularly governments and commercial firms. Certainly, the privacy of data has to be protected fundamentally by laws and regulations as well as the standards [1].

3. CURRENT SOLUTIONS

The solutions to gaining back control of data are numerous, and they have varying levels of strengths. The encryption of algorithms is a better solution compared to the isolation since relies on the users encrypting their data using arbitrary encryption methods. On the other hand, third-party auditing is more secure compared to access controls since a professional auditor in the sector is involved. Cryptography thought it is a developing technology seems to be more secure considered it is dependent on the hash function compared to the isolation strategies that are fond of malicious attacks *on* the VMMs.

3.1 Encryption of algorithm

Data confidentiality is likely to be lost upon hosting in the remote cloud service. Garfinkel, a cloud expert, states that maintaining data confidentiality for clouds such as the Amazon has poised to be a security problem [5]. Encryption algorithms come in handy in combating issues pertaining *to* losing control of data hosted in the cloud architecture [12]. This means that sensitive information is encrypted with private keys known by the CSUs only. Some of the best encrypting methods include the asymmetric and symmetric ones. The provider of the keys is the only fundamental problem facing this technology, but lately, the homophobic encryption has resolved it. The cloud users may rely on the cloud provider for the keys or the arbitrary encryption strategies, and manage the keys themselves [5]. Certainly, an encryption algorithm has become a fundamental way of maintaining the confidentiality of information. This is realized through the use of key distribution, which acts as one of the key strength of this strategy. The keys strengths are based on their length, and the longer the key is, the more secure the data becomes and the vice versa [19].

The RSA algorithm, named after its inventors, Rivest, Shamir, and Adleman is another security algorithm used to secure data in the cloud. It is a common public key algorithm, which employs the necessary decryption, and asymmetrical algorithms. This means that the public key is distributed to all the CSUs for them to ensure their data is encrypted. In addition, the key remains private and everyone does not share it for purposes of data decryption. The RSA algorithm is an adamant and attack proof strategy that provides security to the data through encryption [11]. Notably, by employing the RSA algorithm, the CSU can only access the data by requesting the CSP to authenticate the information and deliver it to the owner. It is worth to note that, RSA is a block cipher; hence, it utilizes integers in mapping all the data stored in the system. RSA works by way of CSPs performing the encryption role and the CSUs doing the decryption using the private key provided [19].

The Advanced Encryption Standard (AES) is also among the most reliable ways of securing data stored and maintaining its confidentiality in the cloud. AES otherwise referred to as Rijindel has recently gained much public traction considering it is an extensively analyzed symmetric block cipher. AES is employed to perform various computer function, but for purposes of securing data in the cloud, it utilizes a 128-bits key length [19]. The CSU is expected to first migrate data to the preferred CSP together with one's service requirements [5]. Upon the uploading of data to the cloud, it is first encrypted using the AES algorithm before being delivered to the CSP. Principally, the key owner is the only one who can access the encrypted information, and it is viewed as a plain text data which is never written anywhere in the cloud for purposes of transparency. Table 1 shows encryption algorithms that used by the most popular cloud service provider.

Table 1: Cloud encryption algorithms

Cloud provides	Encryption algorithm	Methods
Microsoft Azure	RSA	Over secure protocol
Google Cloud platform	AES256 or AES128	Distributed file system and storage device
Amazon "AWS"	AES256 operations	KMS customer master key

3.2 Design a Personal Access Control

Cloud users may be provided with the option to design their personal access control policies in an effort to regaining control of data [13]. It is a strategy that is currently being developed by cloud experts and the progress made has been encouraging. This will provide the cloud user with privileges of a fine-grained level with regard to acting on an object. The cloud service providers should be in a position to resist the malicious attacks by insiders effectively. Markedly, authorization and authentication models can be developed with regard to public clouds. The multi-tenancy nature of these clouds makes it compulsory for the user to be involved in designing the policies. Indeed, this will limit access to the virtual and physical resources to authorized users only. This will be useful in cases where the administrator in possession of hypervisor token is the only one with the powers to launch a hardware [5].

Notably, personal access control systems have varying levels of weaknesses which make the data stored risk from being accessed wrongfully. Some access controls mechanisms are flawed in the sense that differential faults analysis is possible. In this situation, an attacker is able to study and analyze the behaviors of the systems by way of injecting the systems with faults. In addition, cache usage attacks are possible while using access controls considering that the attacker can opt to measure the CPU cache usage on its physical system to screen the co-residents activities [8].

The access controls are often intended to regulate external access into the cloud. They operate by way of governing the object intended actions regardless of whether it is accessing certain information, query issuance, computation analyses among others. Fundamentally, controls are 'principal focused' meaning that control policy managing an individual action is defined to regulate parties responsible for an action and enforce when they try to take action [14]. Authorization and authentication are the two most important aspects of access control in cloud computing. Authentication in this context is defined as figuring out of the principal. Authorization is subject to the former in the sense that upon identification, the process of figuring out their privileges and rights ought to follow. Subject to cloud computing, authorization policy is enforced as a principal attempt to take action, which is based on the rights and privileges of the object [19]. Remarkably, access controls are subject to the CSP policies, but often includes capabilities, role-based access controls, and access control lists among many others [14].

Bringing back control of the cloud to the relevant parties is however faced with some challenges in relation to access controls. Firstly, the contextual nature of access controls in the sense that people are generally allowed to access data that is concerned with themselves alone. This is disadvantageous to the users particularly with respect to information found on the internet of things (IoT) cloud [11]. With the exception of the extremely private data such as medical history and banking details, some other types of information can be considered to fall into the 'break-glass policy' [11]. This is intended to enable flexible access control policies subject to different parties' definitions. Remarkably, access controls regulate the interactions between the CSUs and CSPs at the interface between them, and the former is no longer regulated in relation to areas visited.

3.3 Cryptographic Strategies

The cryptographic strategies are regarded to be among the best ones in addressing the problem of losing control of data [14]. It is a safe method of transmitting and storing data in a certain form so that only the intended individuals can process and read it. Issues related to questioning data integrity can be tackled with the use of the hash function, which is based in local memory. The recalculation of the data received is juxtaposed with data stored locally to aid in authenticating responses by the server. Sirius, a software, is one of the hash function implemented by a significant number of system prototypes associated with data storage. Retrieval of the user's data is addressed by some prototypes such as Proofs of Data Possession (PDP) and Proofs of Retrievability (PORs) [5].

This new system of protecting data has not yet been thoroughly analyzed with the view of highlighting the inadequacies. However, due to its similarity with the algorithm's encryption, the process of authenticating data by the servers may be distorted during attacks thereby jeopardizing the safety of data stored. Notably, a disruption of the local memory, which may result from technical hitches, would result in the breakdown of nearly the whole system, which would lead to distortion of confidential data [8].

The Proof of retrievability (POR) is a scheme, which makes it possible for a (prover) or backup service or an archive to give a clear evidence concerning a CSUs (verifier) capacity to have target file retrieved [5]. Particularly, it is intended to ensure that data files are retained and consistently transmitted by the archives in their sufficiency for purposes of their full recovery by the CSU [16]. Essentially, a POR is often regarded as a Proof of Knowledge (POK) cryptographic model, which is particularly developed to engage 'bitstring' otherwise identified as a large file. Unlike the POK, the POR does not make it a must for the CSU to have the knowledge of the target file [5]. The already existent cryptographic techniques play a vital role in helping the CSUs retrieve files that are of high integrity as well as privacy. In addition, the cryptography technique gives an opportunity for the CSUs to ensure that before files are retrieved, they are neither modified nor deleted by the archives [20].

The POR strategy proposes for the employment of a single cryptographic key, which protects the stored data integrity in its entirety [5]. The protocol works by way of encrypting CSU transferred information and embedding it with Sentinel, which refers to check blocks sets whose value is determined in a random way. The CSP is often challenged by the verifier by way of the former identifying the particular Sentinels collection positioning and probing the latter to bring back the related sentinel values. Notably, in case a sizeable file is either deleted or modified by the CSP, then it is very likely that the number of sentinels would be suppressed. Scholars such as Atiense came up with a very effective and secure Provable Data Possession strategy that observes in full a key cryptography that is symmetric and devoid of any bulk encryption. Fundamentally, the CSUs should ensure that every data block set is subjected to verification tokens particularly before outsourcing begins [21].

3.4 Third Party Auditing

Third-party auditing is a common practice associated with information systems, which has proved to be a productive way of enhancing data security. Both the parties affected by the problem of losing data control should be excluded in the auditing process apart from availing information to the auditors. The auditors' primary focus is data confidentiality both when it is in a stationary status and transit. The auditors assess the cloud service provider overall security management practices in reference to addressing the control problem. It is highly recommended for the auditors to use a combination of CSU or CSP encryption and Message Authentication Codes (MAC) [6][8]. Third-party auditing is a strategy regarded by cloud experts as attack proof though it has some flaws within itself. Nonetheless, one of the strengths associated with TPA is that the auditor is not allowed to introduce additional online burden to the cloud user, and at the same time, TPA does not have access to the copy of the local data. Secondly, the process itself lacks the capacity to introduce new vulnerabilities in relation to the user data privacy. On the contrary, in some instances, the TPA may opt to give a distorted report about the integrity of accurate data during cases where the hash function becomes compromised [16]

Continuous Auditing is another technique, which is encouraged for the purposes of ensuring that the auditors are up to date with the security situation of the data stored in the cloud. It makes it possible for the auditors to react to events or changes immediately over and above updating their auditing reports based on the latest happenings. There were some interesting findings realized from a report by Murthy and Groomer (1989) regarding the implementation of embedded audit modules in the context of usage of control and monitoring layers. Notably, it spawned a stream of research findings in relation to continuous auditing [3].

It is advisable that the auditing methodologies applied to have the capacity to enable auditors to verify the integrity of the data received from multiple CSUs in a simultaneous way [8]. The verification enables the auditors to detect any mischievous and falsifying activities affecting a particular set of data. As a result, immediate action can be taken including denial of access, which would be included in the final auditing reports. In addition, securing data in the cloud would ask for an intensive audit logs analyses for purposes of assuring compliance with regard to data location.

Third Party Auditing (TPA) is a technique that is designed to figure out the stored data integrity, which is often dynamic in nature. It works by eliminating the involvement of the CSU with regard to establishing whether the day stored in indeed intact [16]. This is a critical aspect of cloud computing since it facilitates the achievement of economies of scale. Nonetheless, services of other data dynamics including deletion and insertion as well as block modification may be considered since cloud computing is not limited to backup data or archives solely. By first figuring out the hitches and impeding security issues associated with direct extensions of prior work's dynamic data

updates; it plays a vital role in designing an elegant verification scheme. Essentially, the module developed targets the seamless integration of the two salient features in relation to protocol design.

3.5 Isolation

Isolation is a countermeasure seeking to address the problem of losing control of data during transit [15]. Attacks are often launched during the resource sharing among incongruent users in a multitenant cloud. The isolation may take the option of segregating the storage, memory, and processing of the virtual machines in the infrastructure as a service. Secondly, a transaction being carried out at the same time by different tenants as well as information and data can be segregated. Isolation can be effected correctly through the use of hypervisors. These are unique pieces of computer hardware, software, and firmware used in virtual machine creation and management. The Xen hypervisor is a classic example created to facilitate isolation [8].

Albeit virtualization being central to cloud technology; isolation procedures pose some levels of security risks. It is always problematic to control the administrator on guest and host operating systems. A majority of the contemporary virtual machine monitors (VMMs) lack the capacity to offer isolation in its perfect state. The VMMs ought to disallow any privileges within the virtualized guest environment, which permits host system interference. Although isolation is advisable for protecting data confidentiality, some vulnerabilities have been discovered in virtualization software. Consequently, these vulnerabilities are subject to exploitation by malicious, local users for purposes of gaining privileges or even bypassing the formulated restrictions [18]

Cloud service provision applies a business model that is subject to economies of scale in the sense that their services work through the sharing of resources [20]. For instance, one physical machine can be shared by the tenants by way of ensuring that their processing is run by different VMs. As a result, CSPs ought to maintain an active isolation between CSUs to alleviate data leakage between them. There are different levels where the isolation can take place including the hardware, VM (hypervisor) and OS (containers) [19].

A good illustration of the technique is by way of leveraging Intel's proposed CPU extensions, namely the SGX [20]. Remarkably, provision of storage services that are subject to isolation levels will make the CSP services to implicitly segregate others resources [11]. Levels of isolation may involve shared data storage software and infrastructure. This would involve shared databases; hence, rely on access technologies that are standardized.

Several aspects may be considered with regard to enforcing isolation as a technique that is intended to bring back control of data stored in the cloud [13]. Isolation in the cache may be performed by certain software-level resource management mechanisms. Notably, the Cache stores information that has already been viewed or retrieved and failure to isolate it might result in its leakage thereby exposing it for modification and even deletion [8]. Besides, processor caches and memory bandwidths may be allocated by proposed hardware level solutions. Cloud users should demand from the CSPs a strict mechanism that is intended to separate the data belonging to them. Essentially, a tenant-ID concept should be introduced to specifically target the data-link layer that steadily isolates, segments, and identify CSUs together with their assets in the cloud [11].

3.6 Optimal Solution

The optimal solution to the problem of losing control of data from a managerial perspective is the encryption of algorithms. It provides both the cloud providers and the cloud users with a more secure and practical way of protecting the data. It will provide the CSPs managers with a service level agreement that will see the system security tightened as well as that of the CSUs stored data. It works through both the asymmetrical and symmetrical strategies to enhance data confidentiality and integrity. The encryption process entails the use of encryption keys to access data hosted in the cloud.

These keys are attack-proof, especially when combined with the compressors. The cloud users have the option to encrypt their data with the help of random encryption strategies. It is worthy to note about the pros of the homophobic encryption method, which provides the cloud providers with the options of error localization and correctness verification of the cloud user's data. The recent developments with regard to encryption have made encryption a grand strategy in regaining control of data stored in the cloud. The improvisation encourages the distribution of the keys among the principal parties including the CSUs, CSP, and third parties [8]. Certainly, an encryption algorithm becomes the best optimal solution for gaining back data control considering that malicious attacks have no way to access the system. In addition, by the fact that the users have the opportunity to design their access control options, it means that they are the only ones enjoying

4. SECURE CLOUD SCENARIO

We explain secure cloud scenario by using encrypted cloud services. Online banking is the most common services are done through the cloud.

The smartphone is used now a day to establish electronic transaction over the internet due to the high-power computation it possesses and large screen it provides to the users, thus, more complex computation are eligible to be implemented on the Smartphone [1,3].

Basically, Smartphone is personalizing users through their mobile number, thus it provides an excellent authentication mechanism by exchanging SMS messages.

The proposed system is composed of two android software modules and one PC based software module, as it is illustrated in figure (1). Android modules are responsible for exchanging SMS encrypted messages to authenticate clients who want to use banking gateway. Banking gateway is a server. Figure 2 shows the data flow of transaction over the cloud.

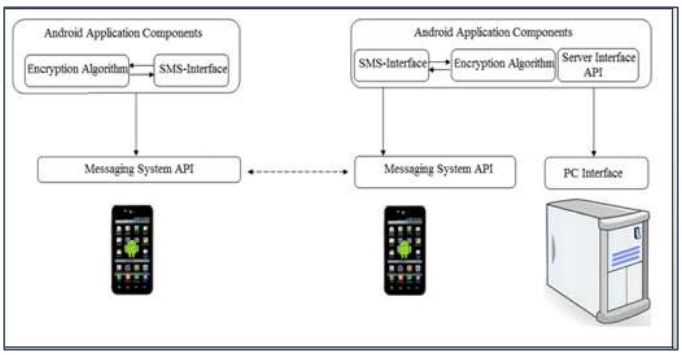

Fig. 1: Android based secure banking gateway system architecture

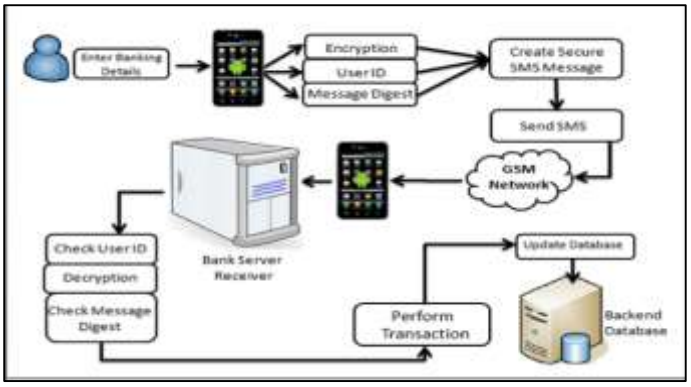

Fig. 2: Data flow in android based secure banking gateway

5. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In conclusion, both an individual, as well as the corporate, will always seek to store their data in a safe and secure platform. Cloud computing technology has come to solve the storage nightmare for a majority of the entities. Nonetheless, losing control over the data is one of the greatest impending problem facing the cloud technology. Remarkably, the problem is complicated by the fact that the cloud is widely accessible to the public; thus, becoming a security threat to confidential data.

Losing control over data is one if the security problem that affects both the CSPs and CSUs. Nonetheless, the problem can be rectified through cryptographic strategies that would see data being transmitted and stored in precise form. Subsequently, this would ensure that only the intended individuals read and process cloud data. On the other hand, loss of control over the functionality stands out as a stern problem affecting cloud computing. This is realized by the fact that the data owners more than often want customized systems based on the needs. However, third-party auditing is a solution that makes it possible for customization of data by way of auditing the overall security management of the cloud.

One of the future events surrounding security of cloud data, which enables the control of the data by an individual, is the introduction of CloudSim. The first advantage of the usage of the application is because of its compatibility with the usage of the cloud services by an individual who can decide on the terms. The process is successful through supporting both the system of dust and the configurations of the user to three essential areas. They include the data registry in the cloud system, connection with the virtual machines through the application, and the policy frameworks as a valuable resource before a user agrees to use the services [17].

The nature of requests in the CloudSim toolkit is flexible through the allowance of extending the utilization of the services. In the case of inter-networked cloud services of computing, the CloudSim toolkit currently only offers a simulation of the nature of the navigation through the services and the modeling aspect of the provisions by cloud (Patel & Patel, 2015). Besides, through the allocation of virtual networks, the CloudSim can help a user get access to custom interfaces that aid in the supply of methods to use and policy implementation. As a result of these services, the CloudSim can be very instrumental in improving the quality of the control of data by an individual.

The best method that that one can use to gather information is through online navigation and virtual responses through the connection to the cloud Inn. Therefore, each will be getting the access to a particular database of the cloud services. When an individual goes to the website through the CloudSim, one can be able to download information from the servers [17].

Experts have continued to exploit the aspect of access control policies in their effort to realize a secure cloud for data. Notably, an individual policy will come in handy in enhancing confidentiality and integrity of data. This will be achieved by establishing an individual policy that would foresee a user design the most preferred way of securing personal data in the cloud. On the same note, businesses and organizations are the biggest users of the cloud services, and a majority of the times they store confidential data, which ask for an attack-proof system

Consequently, the business consumers of the cloud service should be left to design their policy with regard to making their data secure. Fundamentally, these are among the very recent developments that seek to ensure organizations data remain confidential, and the CSPs live to be trusted [22]. Both the individual and the business policy are then reviewed and their strategies incorporated together in designing secure access control policies.

Profile-based access control strategy is an option with high capacity to make cloud computing environment tight secure based on the access control list (ACL) concept. Conventionally, incoming traffic was filtered by the ACLs based on the IPv4 addresses over and above an access matrix based on predefined rules. In the near future, instead of the IPv4 addresses, the rule identifiers and the profile attributes would be incorporated together.

A rule identifier works by hinting to the dictionary where every CURD (create, update, retrieve and delete) operations are identified for every single system in the service as well as each profile. Upon the validation of the user, a service access token is generated by the system, which is then shared with both the resources provisioning service and the user as well. Essentially, this mechanism maps the CSUs to the resources and services available on the cloud over and above minimizing authentication requests [22].

Losing control over access is another significant problem with cloud technology, which is realized by the fact that the cloud is accessible to the public. However, control access policies is a means that works to rectify this problem by ensuring only the authenticated individuals reach particular information. Fundamentally, the problem of losing control in its entirety is sufficiently solved by encrypting algorithms, which is an optimal solution. It works to resolve the control issue from both the managerial and technical perspective. New research direction should be a focus on new security techniques that able to work under a cloud platform such that, blockchain method and techniques. Apply more security algorithm with hybrid and good version.

6. REFERENCES

[1] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107. Retrieved from

[2] Krishna, S. R., & Rani, B. P. (2017). Virtualization Security Issues and Mitigations in Cloud Computing. In Proceedings of the First International Conference on Computational Intelligence and Informatics (pp. 117-1\28). Springer Singapore.

[3] Lins, S., Schneider, S., & Sunyaev, A. (2016). Trust is good; Control is better: creating secure clouds through continuous auditing. IEEE Transactions on Cloud Computing. Retrieved from

[4] Rajkumar, M. N., & Kumar, V. V. (2016). Cloud Computing and its Security perspective. World Scientific News, 41, 51. Retrieved from

[5] AlZain, A. M. (2013). A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds. Journal of Software, 8(5); 1068-1078.

[6] Jaeger, B., Kraft, R., Luhn, S., Selzer, A., and Waldmann, U. (2016). Access Control and Data Separation Metrics in Cloud Infrastructures. 11th International Conference on Availability, Reliability, and Security, IEEE. DOI 10.1109/ARES.2016.9

[7] Li, X., Tang, S., Xu, L., Wang, H., and Chen, J. (2017). Two-Factor Data Access Control with Efficient Revocation for Multi-Authority Cloud Storage Systems. IEEE Open Access Journal, 4; 393-405.

[8] Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., and Vasilakos, A. (2015). A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. Journal of Computing Science and Engineering, 9(3); 119-133.

[9] L. Qian, Z. Luo, Y. Du, L. Guo, Cloud computing: An overview, in Proceedings of 1st International Conference on Cloud Computing (Beijing, China, 2009), pp. 626–631

[10] E. Z. Milian, M. d. M. Spinola, R. F. Goncalves, and A. L. Fleury, "Assessing Challenges, Obstacles, and Benefits of Adopting Cloud Computing: Study of an Academic Control System," in IEEE Latin America Transactions, vol. 13, no. 7, pp. 2301-2307, July 2015.

[11] J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for the Cloud-Supported Internet of Things," in IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269-284, June 2016.

[12] Belapurkar, A., Chakrabarti, A., Ponnapalli, H., Varadarajan, N., Padmanabhuni, S., & Sundarrajan, S. (2009). Distributed systems security: issues, processes, and solutions. John Wiley & Sons.

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

[14] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009, November). Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 85-90). ACM

[15] Tripathi and A. Mishra, "Cloud computing security considerations," 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, 2011, pp. 1-5.

[16] Meenakshi, K., & George, V. S. (2014). Cloud server storage security using TPA. International Journal of Advanced Research in Computer Science and Technology.

[17] Patel, H., & Patel, R. (2015). Cloud Analyst: An Insight of Service Broker Policy. International Journal of Advanced Research in Computer and Communication Engineering, 4(1), 122- 127.

[18] Rai, R., Sahoo, G., & Mehfuz, S. (2013). Securing software as a service model of cloud computing: Issues and solutions. arXiv preprint arXiv:1309.2426.

[19] Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. International journal of engineering research and applications, 3(4), 1922-1926.

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

[21] George, R. S., & Sabitha, S. (2013). Data anonymization and integrity checking in cloud computing. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on (pp. 1-5). IEEE.

[22] Naushahi, U. M. A. (2016). Profile-Based Access Control in Cloud Computing Environment with applications in Health Care Systems. Umair Naushahi.

