Research on key security strategies of cloud computing

Article · September 2018

CITATIONS
0

READS
427

3 authors, including:

Saif Addin Rubaee
University of Anbar
12 PUBLICATIONS **1** CITATION
SEE PROFILE

Shokhan M. Al-Barzinji
3 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Journal of Theoretical and Applied Information Technology
30th September 2018. Vol.96. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RESEARCH ON KEY SECURITY STRATEGIES OF CLOUD COMPUTING

[1]Saif Al-din M. Najim, [2]Shokhan M. Al-Barzinji
[1, 2] College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq
E-mail: [1]sayf73@gmail.com, [2]shokhan_albarzinji@yahoo.com

ABSTRACT

The platform of Cloud computing is model based on Internet environment which enables an easy on-demand access and usage payment of each access and utilization of pool of networks that is shared among multiple users. This type of computing is considered as another innovation that fulfils users' needs and requirements for resources of computing like stockpiling, systems, administrations and applications as well as servers. Securing the cloud's stored Data is seen as one of the significant principles with many challenges and concerns in the research of cloud computing. This study has reviewed the research in a critical manner which focused on the types of cloud computing, industries, deployments and models of delivery. This constant issue is becoming more impactful because of the emerging challenges in cloud computing technology management. From the client's point of view, the security in cloud computing is hazardous, typically in the matter of assurance affirmation problems and securing the data. These problems create shortcomings that hinder the adoption of cloud computing administrations. This paper inspects and illustrates the critical issues of cloud computing in relation to the privacy and protection on the Cloud. Lastly, this paper is concluded with a review to the literature stated as well suggesting on-going future studies.

Keywords: *Cloud computing, Data security, Data privacy, Cloud Cryptography, Security threats.*

1. INTRODUCTION

Cloud computing (CC) is an ideal and convenient model for systems that are obligated to access a shared pool of processing with configurable assets. It can also be swiftly provisioned and discharged with minimal management efforts [1]. Cloud computing can possibly be regarded as a parallel and distributed system of computing which contains a visualized, collective, and interconnected system that is dynamically monitored. This archetype is displayed as one of numerous unified computing resources based on the Service Level Agreements (SLA). This agreement is established between the providers of service [2]. It is a style of computing wherein IT-related capabilities are considered as a "Service" provided to consumers instead of being regarded as a web-derived item. The essential aim of CC is to provide multipurpose and cost-efficient solutions in situations where high-quality services are needed. Most cloud-based application designers invest a great effort in trying to adapt and establish security. In some cases, designers may not be able to give a basic organization towards full security with the current serviceable technological capabilities [3, 4]. The development of CC integrates different parts of the cloud cooperating with each other and forming various data which helps customers to get their needed service at a faster rate. Cloud computing is focused on both front and back ends. The front end is the consumer or the client that requires the service (data or information), while the back end is the multiple devices for information storage and the servers which create the cloud platform [5].

This paper presents a study on the categorization of cloud service-related security challenges, focusing more on cloud service models (SaaS, PaaS, IaaS), identification of the major susceptibilities in cloud systems, and examining the major cloud computing-related challenges documented in the literature. Any potential attack that can result to information or resource misuse is considered a threat, while vulnerabilities refer to system activities that facilitate a successful attack execution. Several articles in the literature have either focused on one service model or on a general listing of cloud security problems without establishing the major differences between threats and vulnerabilities. This study presents a catalog of threats and vulnerabilities, and similarly indicated cloud service models that each type of threat can affect. Furthermore, the study described the ways these vulnerabilities can be exploited to ensure a successful attack execution. Some countermeasures towards resolving these threats or towards improve the identified issues were also presented.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This paper is structured as follows: Section 2 posed the related work, while Section 3 introduced the concept of cloud and provides a point of interest elaboration on Security in the cloud industry. Next, Section 4 demonstrates the newly utilized security solutions for data security and privacy protection. Section 5 presents the recent implemented security solutions. Finally, Section 6 concludes this study.

2. RELATED WORKS

In recent times, cloud computing security has attracted much attention and has gained much investment interest in commercial enterprises. Cloud security alliance covers a wide area of security for significant cloud computing areas of interest. Additionally, the abnormal state of security issues in cloud computing models, such as payment, integrity of information, and protection of personal data has been investigated [6]. Bernd et al. [7, 8] enumerated the vulnerabilities of cloud computing security those of cloud attributes, innovation, and security controls. Furthermore, Subashini et al. [9] examined the security challenges in cloud service delivery models, focusing more on the SaaS (Software-as-a-Service) delivery model. Some studies have identified the issues in cloud computing security. In this paper, a comprehensive investigation of the security challenges in cloud computing is carried out, focusing more on the deployment varieties and cloud service delivery models.

Moreover, many researchers have stated cloud computing benefits based on support cost-saving [10], scalability [11, 12], availability [13, 14], innovation [15], speed efficiency [16, 17], easy management and disaster management [18]. Table 1 illustrates benefits offered by cloud.

Nevertheless, several cloud computing-related security issues have been studied, but in this work, some of encountered security issues in cloud computing were detailed, focusing more on the deployment of cloud computing as well as the types of service delivery. Nevertheless, a security model is suggested in order to provide integrity and confidentiality to the user data in cloud computing environment.

Table 1: Cloud computing benefits

Benefits	Clarification
Availability	Due to the scale ability, the cloud provider can offer high availability.
Scalability	Cloud service enable the rapid adaptation of IT for enhancing business needs.
Innovation speed	Comparing to traditional IT schemes, cloud services can be provisioned with just few hours' notice, rather than weeks or months.
Easy management	Infrastructure maintenance, software or hardware is simplified.
Efficiency	The existence of an effective IT can enable institutes to concentrate on their major business and invest into innovative researches. Cloud services does not only contribute substantially to organizational growth and competitiveness, but can help them to maximize their financial gains.
Cost saving	The organization can be highly decrease spending on IT resources with the cloud usage.
Disaster management	In case of disinters, an off-site backup is always helpful. Keeping crucial data backed up using cloud storage services in the need of the hours for the most of organization.

3. CLOUD COMPUTING

In this area we will research the cloud computing from three angles including its essential and vital qualities, delivery models and deployment models, as demonstrated in Figure 1.

3.1 Understanding of cloud computing

Cloud can be referred to as a virtual collection of computing resources which can perform the following functions:

- Can manage a range of workloads, such as user-oriented interactive applications and back-end operations.
- Can quickly deploy more resources in case of increased workload through quickly deploying more physical or virtual machines.
- Can support self-healing, redundancy, and highly scalable model; so, the workload can be recovered from several unavoidable software or hardware failures.
- Can monitor the usage of resources in real-time; can also rebalance the resource allocation whenever there is a need.

Cloud computing is a model consisting of several service models [19] as listed below:

Journal of Theoretical and Applied Information Technology
30th September 2018. Vol.96. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

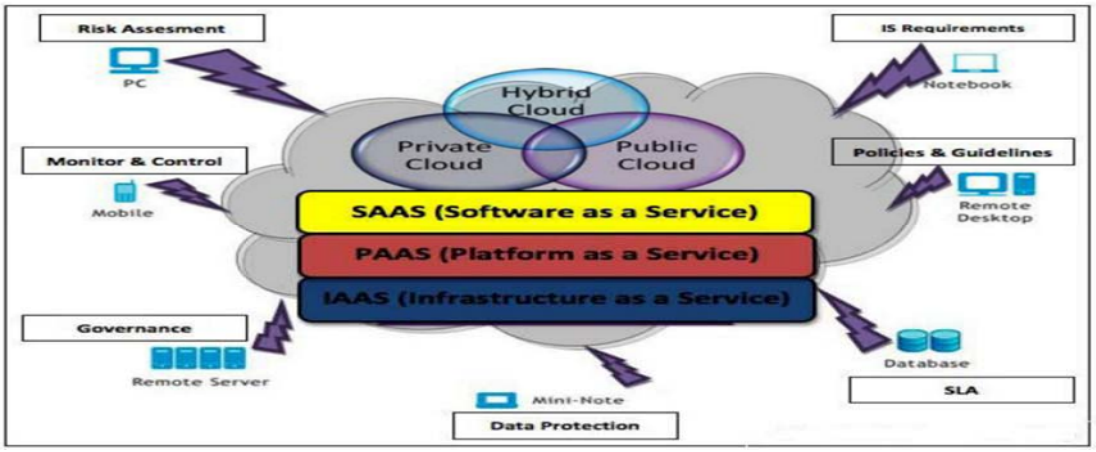

Figure 1. Cloud deployment model [20]

- Infrastructure as a service (Iaas): It provides a platform virtualization environment as a service instead of client purchasing software, network equipment or data center, although these resources are fully outsourced.
- Software as a service (Saas): It can provide different users with access to the application. Software is provided to the customers as a service based on their demand. Buyers are empowered to use licences available on the cloud server.
- Platform as a service (Paas): Here, cloud computing provides development environment as a form of service. The infrastructure of a middleman can be utilized to develop a personal program that can be delivered to the users through the servers over the internet.

3.2 Cloud computing deployment model

Security challenges begin with the models for cloud service delivery. There are 4 types of models deployed in cloud computing [20].

- Public cloud: A public cloud depicts the conventional cloud computing where resources are dynamically monitored on a self-service basis over the Internet. This is done by implementing a third-party service provider that offers and share bills and resources via a registering utility basis. This cloud service focuses on a pay per usage model similar to the metering system for power and electricity, making it very flexible and adaptable, thus, attracting more demand for optimizing low-security levels compared to other cloud models [21]. This is due to the extra effort in ensuring the security of all applications and information on the public cloud.
- Private cloud: A private involves the use and control of cloud infrastructure in a personal/private cloud. It is mainly hosted in the central database of a firm and managed by either an internal person or a service provider. The advantage of this model are the individual controls the security of the system, Quality of Service (QoS), as well as compliance [20].
- Hybrid cloud: A hybrid cloud is a mixture of several cloud infrastructures (such as a private, public or community cloud infrastructure) which maintains the distinctive nature of its entity, but still connected through a standardized technology that allows data and application proprietary [1].
- Community cloud: This is a collection of cloud infrastructure pooled by several administrators and provides support to communities with mutual concerns such as policy, consideration, security requirements, and compliance.

3.3 Cloud security industry

To avoid encountering security issues that could be dangerous to the cloud system, the composition of the cloud security sector must be sorted. The 3 aspects of the cloud security sector as follows:

i. Cloud vendors: Several cloud service providers like Amazon, Microsoft, and IBM provide solutions for cloud computing security deployment to improve the security of such platforms with respect to service continuity, service competency, and user data security. Most of such solutions may depend on ID audit, encryption data, and ID authentication identification [22, 23].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ii. Operators: From the perspective of an administrator, there are 2 major approaches in securing cloud computing. One of the approaches is to achieve a central control on the platform by combining the current security system with a cloud computing infrastructure. The second approach is to develop cloud computing security services and make them available to clients as obtainable in some network operators that are already using such aspect [24].

iii. Security vendors: These are the established IT security solution vendors in the cloud computing space. They offer their own cloud computing products and solutions. There are evidently two cloud perspectives; one is based on the server perspective and the other based on the client perspective. The server-based perspective basically attempts to ward-off established server threats before they reach the client. This is achieved by creating an enormous lists system. The client-based perspective mainly works on the traditional approaches [23, 25].

For the afore-mentioned cloud security rules, the operators can still strive for cloud security. Thus, to provide security services to customers, operators must work with the security vendors to ensure the provision of providing apparatus and services. This can be achieved by exploring the benefits of the network operators and those of data encryption, ID authentication, and audit solutions offered cloud vendors. Hence, they can offer end-to-end security solutions in the cloud computing platform.

3.4 Challenges in cloud computing

There are several challenges in cloud computing which are necessary to keep in knowledge. Some of challenges are given as bellow [4, 26, 27]:

- Access control: this is considered to be an issue for all service providers in general, which could lead to issues in security through revealing user's data and provide the hackers an opportunity to gain access to the infrastructure of the organization [28].
- Accounting: is a critical aspect that must be measured in installing a service in the solutions of cloud computing to maintain an efficient management of the network [29].
- Compliance: Cloud computing lacks point of supporting the methods to manage the compliance management of its solutions. That may create dangerous issues in securing the data and privacy [30].
- Cross-Organizational Security Management: this is an enormous challenge when it comes to cloud computing in order to attain and maintain the requirements of security and compliance with security-level arrangements which need to function among organizations to guarantee attaining the appropriate security requirements in cloud computing [30].
- Extensibility and Shared Responsibilities: the users and service providers must be attentive regarding the security issue in cloud computing. Up to now, it is not clear on how the responsibilities for security will be done in cloud computing [31].
- Heterogeneity: its role comes in at time when different service providers convey a great number of services through different technologies, that may create issues in heterogeneity, it could happen as a result of incompatibilities in hardware or software level [32].
- Identity management (IdM): It is a critical feature in security of cloud computing, its aim is to perform the validation and verification process between heterogeneous clouds services, although it still has some problems related with interoperability between the current security technologies [33].
- Integration: when organizations or customers require implementing multiple providers of the service for whatever reasons, they will require implementing and integrating software and data in several clouds. This may resolve some cases when using hybrid clouds is intended [34].
- Performance: using Cloud computing could reduce the cost, yet the performance issues such as communication time between users and the cloud services is becoming problematic, due to the number of users increase, the amount of the information and the data that going to be transfer to the user's increases, which it causes high load on the hardware and software. One other element is the distance between the service providers and the users which makes a difference. In addition to that, the customers may scale up their cloud infrastructure beyond what was expected, in this case it is considered to be serious issue to the service provider [35].
- Requirements of the Bandwidth: prior to the implementation of a cloud service, the organizations must evaluate the communication bandwidth requirements and assess the services

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

with respect to large amounts of data transmission [36].

- Provision: cloud computing is based on service provisioning, there is huge demand in using provisioning throughout cloud services and activities either in public or private infrastructure [37].
- Risk management and analysis: this is also an important key feature in the cloud security. It is regarding decreasing the load capacity in cloud computing through scanning and identifying any threat in the service before providing it to customers [37].
- Service Level Agreement (SLA): it is a contract between the cloud service providers and the users which is about the provided service level agreement for the use of service, and the method of delivering the service for the users [38].
- Virtualization: it is the manner of delivering services in the cloud to the customers, especially when it IaaS services, although it still suffers from issues [39].
- Policies: cloud computing requires well- written policy for the security procedures and guidelines that is the implemented in the solutions [40].
- web browser Security: the security requirements in the web browser is not enough to handle the users' needs of a sophisticated and complex banking and critical environments for a shared solution such as cloud solutions [41].

3.5 Attacks and threats in Cloud computing

The Cloud computing is basically a method of accessing platforms, services and resources for a certain organization. On the other hand, hackers, attackers and security researchers found out that cloud computing is not entirely secure. It has some problems and they can be elaborated on below [28, 42]:

- **Service and Account hijacking:** one of the most dangerous security threats, it occurs when the attackers intend to hack a web service in a website hosted in a service provider or cloud server then install their control software in the cloud provider infrastructure [43].

- **Nefarious use and Abuse and of cloud computing:** in this type, the attacker uses the cloud computing power of the cloud infrastructure to attack his target using malware and spam such as botnet.

- **Backdoor Channel attacks:** this type of attack occurs in IaaS, when giving an effective user's high permeation in the VM's or the Hypervisor level. This may affect the service availability and data privacy.

- **Cross site scripting attacks**: also called XSS attack, it is one of the most impactful attacks on security weakness found throughout the web applications. One of the most wide range scripting is Java script language that is commonly used in such attack [44].

- **Cloud malware injection attack:** this is listed at the top in the cloud computing security list of attaches, where it purposes to inject macules application, virtual machine or malwares to the cloud infrastructure.

- **Denial of Service (DoS) attacks:** In this kind of attack the service will seize to be available when the users intended to request it from the server. They normally receive error 404 meaning the service is not found [45].

- **Insecure application programming interface:** this type is when the service providers deliver the service to the customers using APIs, the APIs have to be encryption, with secure authentication, provided with secure access control, and activity monitoring mechanisms.

- **Man in middle attacks:** In this type of attack, the hacker creates an autonomous connection between the the service provider and customer to observing the data and information for the service without them knowing.

- **Metadata spoofing attack:** In this type where the web services providers send the service metadata document to the client system, which contains all information regarding the service request such as message format, security requirements, location of network … etc. In this case the goal of attacker is to reengineer the web service metadata descriptions, demanding to change the network references and endpoints to the policies of security.

- **Malicious insiders:** this kind of security threat occurs when there is a lacking in the security concern for how to access the service provider from employees to the virtual properties of the cloud. This threat may be more complex due to employee's privilege lack implementing in the cloud system. Also, updated the responsibilities when their behavior or jobs is changed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- **Phishing attack:** it's about effecting the user privacy and it's data and information that is exposed by allowing users to access fake web link installed in their PC's Malicious codes exposed that data.

- **SQL Injection attacks:** This kind of issue happened when hackers try to attacked website database through the code injected in SQL statements using the website inquiry methods that can be deactivates a security in a website.

- **Shared technology's vulnerabilities:** normally, cloud computing utilizing the same infrastructures used in the internet. That's shared among the cloud customers. Thus, all the problems that are currently in the Internet infrastructures going to be migrate to the cloud. In other way, the traditional components have not developed to sharing it is resources such as in cloud computing systems.

- **Sniffer attacks:** In this of type attack, attacker wants to read the content of the network packet whereas there is no encrypted methods have been applied during the sending of it. Sniffer could be a script, an application or a device.

- **Unknown risk profile:** this kind of security threat happen as a result of making attention on the functionalities and the features that gained from the implementing cloud services without making any consideration for the security technologies and producers that going to be developed. Which the features may have access to the data from third-party and this data may disclose for any reason.

- **Security concern with the virtual machine Manager:** In this type of security concern the service providers have to be very careful, on the services provided by the VM technology to the users because this type off technology suffer from some security level in some cases.

- **Zombie attack (DoS/DDoS):** it cased through indirect/ direct flooding to host in the Hypervisor, Network, or VM level. May affect service availability. Also may create an user account for false service usage.

From the review attacks above, the user protective security requirements as mentioned in table 2.

3.6 Privacy issues in cloud

Clients are connected to networks via server-oriented services, and all server-related processes must be complete on the server. Server computing entails that all client-related data be stored in the server (also called a data center). But there could be some privacy-related issues, and some of these issues are discussed in this work [46]:

- Loss of Control: A cloud user makes use of some cloud-based applications. These applications are used to make documents and projects which can also be stored in the cloud. Client that needs to switch cloud service provider can be threatened with the abuse and manipulation of his private information presently stored in the cloud data centre.

- Access Control: Client's data saved on the cloud may not be accessible to him over time form some reasons. This data can be accessed and manipulated by an unauthorized person due to the lack of authorized access control rights.

- Data Boundary: Client's data can be duplicated by the cloud providers to serve another client at another location. This data will always be available for use when required because it is duplicated. Stored data that has not been used over time can be deleted from the data centre, and several copies of server data can result to information leakage.

- Invalid Storage: Due to financial reasons, data can be inappropriately stored in the cloud since authentic data storage demands extra charges from the cloud provider, and this could reduce the cloud provider's gain. So, this could be considered a serious data privacy issue in cloud computing.

4. RECENTLY IMPLEMENTED SECURITY SOLUTIONS

IBM has recently created a fully homomorphic encryption scheme [47]. These homomorphic encryption schemes have a significant influence on cloud computing. Considering the cloud service providers analytical service, IBM uses homomorphic encryption schemes to encrypt the data; complex scientific operations are executed without tampering with the encryption.
With this method, the encrypted information can be processed without being decrypted. Roy and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ramadan joined a Decentralized Information Flow Control (DIFC) with different mechanisms for privacy protection, transforming them into information generation before calculating the stages and establishing a system called Air Vat for privacy protection [48]. This system helps to avoid the privacy leakage without an approval from Map Reduce figuring methodology. The major problem in most encryption processes is key management. A great knowledge is needed to manage the keys that are not available to the user. Such issues can be solved using Key Management Interoperability Protocol (KMIP) and Organization for the Advancement of Structured Information Standards (OASIS).

Table 2: Security requirements specification

Concerning the verification of information integrity, a check must be carried out due to data exchange, time, and data transfer cost. The users may not know how to upload after verification. Regarding checks for information integrity with respect to information correspondence, time cost, and exchange expenses, the users may not be able to first download the information in order to ascertain its accuracy before transferring the same information. The information in the cloud is dynamic, and conventional solutions for information integrity checks are no longer applicable.

Level	Level of Service	Users	Security requirements	Threats
Phsical	Physical datacenter	Owner relates to a organization or person which possesses the infrastructure upon which clouds are deployed	• Hardware reliability • Hardware security • Network protection • Legal not abusive use of cloud computing	• DDOS • Connection flooding • Misuse of infrastructure • Hardware modification • Hardware theft • Network attacks • Natural disasters
Virtual	Infrastructure as a service (IaaS) Platform as a service (PaaS)	developer–Moderator applies to an organization or an individual or deploying software on a cloud infrastructure	• Application security • Secring the Data (data at rest, data in transit or remanence) • Secure images • Cloudmanagement control security • Communication security • Virtualcloud protection • Access control	• Software modification • Impersonation • Software interruption (deletion) • Traffic flow analysis • Seasion hijacking • Defacement • Network Exposure • DDOS • Connection flooding • Disrupting communications • Impersonation • Programing flaws
Application	Software as a service (SaaS)	End users relates to an organization or an individual which subscribes to a service provided by a cloud provider and is liable for its use	• Privacy in multitenant environment • Communication protection • Data protection from exposure (remnants) • Service availibility • Software security • Access control	• Alteration and data at transit and rest • Breach in Privacy • Data interruption (deletion) • Seasion hijacking • Impersonation • Exposure in network • Traffic flow analysis • Interception

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

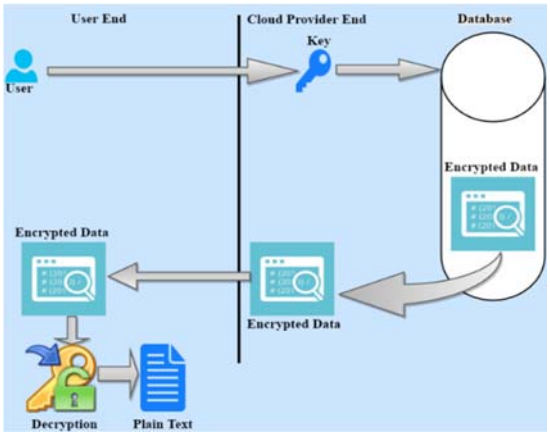

Figure 2: Data Decryption process

Many studies have been proposed on security in recent times. Different researchers have operated proof of identity-based cloud computing security model [49]. But the identification of only specific user does not prevent data hacking or stop cloud database intrusion. Yao's Garbled Circuit has been deployed for data security in cloud servers [50]. It is also dependent on work identification. Advanced encryption standard (AES)-based schemes for file encryption are applied in most of these models [51], but these models are designed to keep both the process of file encryption and the encrypted file in one server.

A successful attack on the server can grant the intruder access to all the information in the server without restriction, and this is unacceptable. Few other models for ensuring cloud security have been proposed [52, 53]. Although the end-user-server connection can be secured by these models, they do not encrypt the loaded information or files. To ensure an optimum security, data must be encrypted before being uploaded to the servers to avoid being tracked. On the other hand, some secured models are also being researched for cloud security [54, 55], but these models do not ensure all the principles guiding cloud computing security [56].

The verification of public data integrity is encouraged by NEC Lab provable Data Integrity (PDI). Cong Wang developed a mathematical model for verifying the integrity of data stored in the cloud. Mow bray developed a tool for Client-based Privacy Management [57] and stated the proposed tool is a user-focused trust model which helps users to have the control of data storage as well as the utilization of most sensitive cloud information. The privacy protection technological issues (such as anonymous, methods for information pre-processing, and graphical anonymization) are encountered when applied to a large amount of data while analysis is carried out using the current solution.

5. DISCUSSION

In case of overcoming cloud security challenges, technical solutions should be considered. In addition to SaaS operators, other cloud computing operators generally have no ability data protection in term of privacy. Therefore, for reducing the threat on cloud computing platforms, enterprise users must adopt the cryptography technology which will provide data integrity by preventing unauthorized access to the sensitive data.

We propose a secure model in order to provide integrity and confidentiality to the user data in case of uploading or downloading from cloud servers, figure 2, explains that how the data stored in encrypted form in cloud's data base server from a plain text at user side. When users want to send a message he supposed to write it in simple text then according to this model user has to encrypt the message or files with the help of encryption algorithm (AES) which is installed at user side, this mechanism secure to the user side which will reduce the chances of the data lose issue and the threats by hacker attacks. The encrypted data will be uploaded to the cloud database and only users with authentication key can access to the files.

Whereas, figure 3 will illustrate how the user can obtain the desired data from the cloud database at cloud provider's end. The user sends the request for the encrypted data along with the key and service provider will check the database for that particular request and if it available in database, the service provider will send it to the requested user. The user now has the encrypted form of desired data. The user has to decrypt this data to get the plain in readable form. Now the user has everything in his own side and this approach will provide high trusted platform by reducing the possibility of unauthorized person to gain an access to the user data on cloud servers.

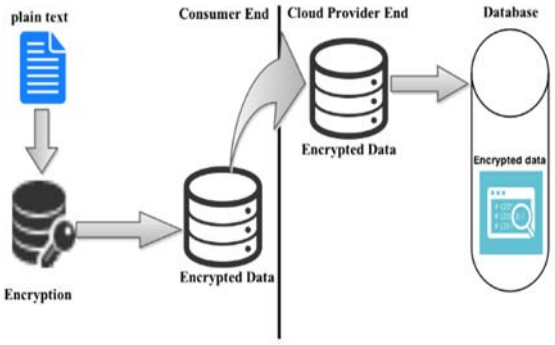

Figure 3: Data Encryption process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This study mainly aims to identify the major privacy and security challenges encountered presently in cloud computing. The study also aims to provide cloud service users with the necessary information on the recognition of the threats associated with cloud services. The study covered two major areas of security and privacy issues, which are: a) a survey of the most relevant security challenges in the existing cloud computing environments and b) analysis of the ways towards addressing these challenges to ensure their elimination in the cloud environment. The identification of these privacy threats will help in providing a secure, dependable, and trusted cloud computing services. The following aspects can be considered in the future studies: a) the use of a quantifiable approach to analyze and evaluate the security problems in cloud computing. The approach suggested in this study is a first step towards the analysis of security challenges in cloud computing, then b) applying the proposed approach in real cloud computing environment.

6. CONCLUSION AND FUTURE WORK

This paper mainly focused on cloud computing security issues. It is important to consider security and safety when utilizing cloud services. The study detailed some of the security challenges, such as information stockpiling and transmission, as well as application security. Also covered were cloud security integrity and the security of identified third-party assets. The likelihood of danger was also discussed to distinguish high hazard risk on the cloud security. The study showed the need to reinforce the security capacities of a clod system to improve its security over the Internet. Cloud computing is not currently fully realized as there is a need for more exploration.

Consequently, security is ascertained as the most vital threat to both vendors and clients of cloud computing. Several researchers, IT security professionals, and vendors are still conducting experiments in this field together with a wide range of models. Despite these serious attempts, there have been no significant solutions to the need of the users and cloud service providers. While exploring the security issues found in cloud computing, there has been no accessible security benchmarks to establish a secure cloud computing. This study will further examine this security aspect and its protocols to ensure a better security while using cloud-computing.

REFRENCES:

[1] Mell P, Grance T. The NIST definition of cloud computing. 2011.

[2] Nemati H, Singhvi A, Kara N, El Barachi M, editors. Adaptive SLA-based elasticity management algorithms for a virtualized IP multimedia subsystem. Globecom Workshops (GC Wkshps), 2014; of Conference.

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

[4] Ahmed HAS, Ali MH, Kadhum LM, Zolkipli MF, Alsariera YA. A Review of Challenges and Security Risks of Cloud Computing. Journal of Telecommunication, Electronic and Computer Engineering (JTEC).9(1-2):87-91,2017.

[5] Li Q, Wang Z-y, Li W-h, Li J, Wang C, Du R-y. Applications integration in a hybrid cloud computing environment: Modelling and platform. Enterprise Information Systems.7(3):237-71,2013.

[6] Abbas H, Maennel O, Assar S. Security and privacy issues in cloud computing. Springer,2017.

[7] Grobauer B, Walloschek T, Stöcker E. Understanding cloud computing vulnerabilities. Security & privacy, IEEE.9(2):50-7,2011.

[8] Khan N, Al-Yasiri A. Cloud security threats and techniques to strengthen cloud computing adoption framework. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications: IGI Global; 2018. p. 268-85.

[9] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications.34(1):1-11,2011.

[10] Al-Badi A, Tarhini A, Al-Kaaf W. Financial Incentives for Adopting Cloud Computing in Higher Educational Institutions. Asian Social Science.13(4):162,2017.

[11] Catteddu D. Cloud Computing: benefits, risks and recommendations for information security. Web Application Security: Springer; 2010. p. 17-.

[12] Satyanarayanan M. The emergence of edge computing. Computer.50(1):30-9,2017.

[13] Ghosh R, Longo F, Frattini F, Russo S, Trivedi KS. Scalable analytics for iaas cloud availability. Cloud Computing, IEEE Transactions on.2(1):57-70,2014.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14] Guerrero-Contreras G, Garrido JL, Balderas-Diaz S, Rodríguez-Domínguez C. A context-aware architecture supporting service availability in mobile cloud computing. IEEE Transactions on Services Computing.10(6):956-68,2017.

[15] Ge J, Wu Y, Li T, Yuepeng E, Zhang C, editors. Experimenting adaptive services in sea-cloud innovation environment. Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on; of Conference.

[16] Mathew T, Sekaran KC, Jose J, editors. Study and analysis of various task scheduling algorithms in the cloud computing environment. Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on; of Conference.

[17] Stergiou C, Psannis KE, Kim B-G, Gupta B. Secure integration of IoT and cloud computing. Future Generation Computer Systems.78:964-75,2018.

[18] Ma Z, Yang L, Neilson RP, Hess A, Millar R, editors. A survivability-centered research agenda for cloud computing supported emergency response and management systems. Aerospace Conference, 2014 IEEE; of Conference.

[19] Boutaba R, Cheng L, Zhang Q. On cloud computational models and the heterogeneity challenge. Journal of Internet Services and Applications.3(1):77-86,2012.

[20] Xu X. From cloud computing to cloud manufacturing. Robotics and computer-integrated manufacturing.28(1):75-86,2012.

[21] Khalil IM, Khreishah A, Azeem M. Cloud computing security: a survey. Computers.3(1):1-35,2014.

[22] Kshetri N. Cloud computing in developing economies. ieee Computer.43(10):47-55,2010.

[23] Ahmed HAS, Zolkipli MFB. DATA SECURITY ISSUES IN CLOUD COMPUTING&58; REVIEW. International Journal of Software Engineering and Computer Systems.2(1):58-65,2016.

[24] Kshetri N. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy.37(4):372-86,2013.

[25] Pavlik J, Komarek A, Sobeslav V, editors. Security information and event management in the cloud computing infrastructure. Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on; of Conference.

[26] Dogra N, Kaur H. Cloud Computing Security: Issues and Concerns. International Journal of Emerging Technology and Advanced Engineering.3(3)2013.

[27] Yang C, Yu M, Hu F, Jiang Y, Li Y. Utilizing cloud computing to address big geospatial data challenges. Computers, Environment and Urban Systems.61:120-8,2017.

[28] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems.28(3):583-92,2012.

[29] Ruiz-Agundez I, Penya YK, Bringas PG, editors. A flexible accounting model for cloud computing. SRII Global Conference (SRII), 2011 Annual; of Conference.

[30] Schleicher D, Fehling C, Grohe S, Leymann F, Nowak A, Schneider P, et al., editors. Compliance domains: A means to model data-restrictions in cloud environments. Enterprise Distributed Object Computing Conference (EDOC), 2011 15th IEEE International; of Conference.

[31] Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences.305:357-83,2015.

[32] Ng WS, Kirchberg M, Bressan S, Tan K-L. Towards a privacy-aware stream data management system for cloud applications. International Journal of Web and Grid Services.7(3):246-67,2011.

[33] Werner J, Westphall CM, Westphall CB. Cloud identity management: A survey on privacy strategies. Computer Networks.122:29-42,2017.

[34] Fortino G, Pathan M. Editorial: Integration of Cloud computing and body sensor networks. Future Generation Computer Systems.35:57-61,2014.

[35] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, et al. A view of cloud computing. Communications of the ACM.53(4):50-8,2010.

[36] Puthal D, Sahoo B, Mishra S, Swain S, editors. Cloud computing features, issues, and challenges: a big picture. Computational Intelligence and Networks (CINE), 2015 International Conference on; of Conference.

[37] Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem. arXiv preprint arXiv:1609011072016.

[38] García JM, Fernandez P, Pedrinaci C, Resinas M, Cardoso J, Ruiz-Cortés A. Modeling service

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

level agreements with linked USDL agreement. IEEE Transactions on Services Computing.10(1):52-65,2017.

[39] Wu L, Garg SK, Versteeg S, Buyya R. Sla-based resource provisioning for hosted software-as-a-service applications in cloud computing environments. Services Computing, IEEE Transactions on.7(3):465-85,2014.

[40] Zhang Q, Cheng L, Boutaba R. Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications.1(1):7-18,2010.

[41] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, et al. Security and privacy for storage and computation in cloud computing. Information Sciences.258:371-86,2014.

[42] Hussain SA, Fatima M, Saeed A, Raza I, Shahzad RK. Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics.13(1):57-65,2017.

[43] Mishra N, Sharma TK, Sharma V, Vimal V. Secure Framework for Data Security in Cloud Computing. Soft Computing: Theories and Applications: Springer; 2018. p. 61-71.

[44] Mahmoud SK, Alfonse M, Roushdy MI, Salem A-BM, editors. A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques. Intelligent Computing and Information Systems (ICICIS), 2017 Eighth International Conference on; of Conference.

[45] Thangavel M, Nithya S, Sindhuja R. Denial of Service (DoS) Attacks Over Cloud Environment. Advancing Cloud Database Systems and Capacity Planning With Dynamic Applications:289,2017.

[46] Joshi B, Joshi B, Rani K, editors. Mitigating Data Segregation and Privacy Issues in Cloud Computing. Proceedings of International Conference on Communication and Networks; of Conference.

[47] Vamshinath N, Ramya KR, Krishna S, Bhaskar PG, Mwaseba GL, Kim T-h. Homomorphic Encryption for Cluster in Cloud. International Journal of Security and Its Applications.9(5):319-24,2015.

[48] I R, HE R, STV S, A K, V S, E W, editors. Airavat: Security and privacy for MapReduce. the 7th Usenix Symp on Networked Systems Design and Implementation; of Conference; San Jose.

[49] Li H, Dai Y, Tian L, Yang H. Identity-based authentication for cloud computing. Cloud computing: Springer; 2009. p. 157-66.

[50] Bugiel S, Nürnberger S, Sadeghi A-R, Schneider T, editors. Twin clouds: Secure cloud computing with low latency. Communications and Multimedia Security; of Conference.

[51] Vaquero LM, Rodero-Merino L, Morán D. Locking the sky: a survey on IaaS cloud security. Computing.91(1):93-118,2011.

[52] Dhole HT, Papade PC, Bhosale SB. Ensuring Data Storage Security using Cloud Computing. Intl Journal of Advance Research in Computer Science and Management Studies.2(1)2014.

[53] Rathi A, Parmar N, editors. Secure Cloud Data Computing with Third Party Auditor Control. Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014; of Conference.

[54] Thuraisingham B, Khadilkar V, Gupta A, Kantarcioglu M, Khan L, editors. Secure data storage and retrieval in the cloud. Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on; of Conference.

[55] Rewagad P, Pawar Y, editors. Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. Communication Systems and Network Technologies (CSNT), 2013 International Conference on; of Conference.

[56] Hamlen K, Kantarcioglu M, Khan L, Thuraisingham B. Security issues for cloud computing. Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies.1502012.

[57] Mowbray M, Pearson S, editors. A client-based privacy manager for cloud computing. Proceedings of the fourth international ICST conference on COMmunication system softWAre and middlewaRE; of Conference.