International Journal of Computing Science and Information Technology, 2018,

SSN: 2278-9669, April 2018 (http://ijcsit.org)

Survey

On

Data Safety and Effectiveness estimation in cloud computing using Cloud Computing Adoption Framework

Jyoti Vaishnav

Department of Computer Application, Presidency College Bangalore

Abstract

Cloud computing has emerged as an important and resourceful platform in which huge amount of data can be stored, and accessed in a secure manner. The data that are accessed and retrieved in cloud computing are prone to several security attacks. The security attacks result in loss of sensitive and confidential data during data transfer. The efficiency of the data being transferred gets affected by these attacks. Numerous research works have been done in cloud computing domain which focuses on secured and effective data transmission. An effective technique which estimates the data safety along with optimization approach is not yet defined. This current research work aims at achieving effective data safety in cloud computing b incorporating Cloud Computing Adoption Framework (CCAF) model. The input data fed to the cloud server undergoes the following process i) gets compressed within the space using CCAF, ii) denoising by deploying wavelet transformation, iii) secured data transfer using Advanced Encryption Standard(AES) key, iv) Dragonfly algorithm and AES provides improvement in the data storage.

Keywords: Advanced Encryption Standard, Cloud computing, Cloud Computing Adoption Framework

1. Introduction

The benefits of cloud computing to both the service providers and the end users have led to rapid adoption of the deployment of online services and applications. As several businesses and individuals increasingly depend on the cloud system, some of the private data is handled and stored on the systems which are outside of their administrative control [1]. The data safety and data confidentiality are the two important parameters which defines the efficiency of the system. The cloud computing is depicted as a collaborative IT (Information Technology) background, which is prearranged by the objective of computable and remotely accessible IT assets for effective and efficient utilization. It is a model for permitting convenient, on-demand network access to a collective pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be swiftly provisioned and unconstrained with nominal management effort or service provider interaction [2]. Five vital features of cloud computing listed by NIST are on demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Mobile cloud computing typically referred as anytime, anywhere user-friendliness to requests and data through internet uses mobile devices [3]. The data safety and data confidentiality are the two important parameters which defines the efficiency of the system.

The Cloud computing has a variety of characteristics, with the main ones being:

- Shared Infrastructure — the shared infrastructure utilizes a virtualized software model, permitting the distribution of physical facilities, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the most of the available infrastructure across a number of users.
- Dynamic Provisioning — the dynamic provisioning permits the establishment of services depending on the present demand requests. This is done spontaneously with the help of modification in software automation, by

permitting the expansion and narrowing of service proficiency that is desirable depending the demand. This dynamic scaling needed to be done while preserving high levels of dependability and security.

• Network Access — the network accesses need to be accessed via the internet from a wide collection of devices such as PCs, laptops, and mobile devices, using standards-based APIs (for example, ones based on HTTP). Deployments of services in the cloud comprise all from using business solicitations to the up-to-date application on the modern smartphones.

• Managed Metering —the managed metering uses metering for handling and adjusting the service and to offer reporting and billing info. In this technique, clients or users are billed for amenities conferring to how much they have essentially used throughout the billing period. In short, cloud computing permits for the distribution and accessible deployment of services, as needed, from almost any location, and for which the customer can be billed based on actual usage.

Cloud computing diminishes assets expenditure (CAPEX) and it compromises high calculating at lower cost. Improvement of hardware/ software requirement is also easy with the cloud, without disturbing the current work [4]. Scalability and maintenance is easy in the case of cloud. Easily user can rent/lease the services offered by cloud computing vendors. User will be charged as pay per usage like utility based services. It is easy to scale if the application is deployed in cloud. It takes away all the risks of managing resources. General Cloud is generous and ensures good performance at lower cost instead of making additional capital speculation. Apart from IaaS, SaaS, PaaS, XaaS is possible in case of cloud. Users will be indicted based on utility computing. Cloud adopts as pay per usage model. Besides having enormous good features like performance, scalability, flexibility, adoptability, cloud has some serious issues like security, availability, etc.

2. Problem statement

The cloud computing has emerged as a wide area of research these days because of its applicability in diverse fields. Numerous research works have been done with respect to cloud computing domain in providing data security, and data safety [5]. This research work focuses on a framework known as Cloud Computing Adoption Framework (CCAF), comprises the summary, rationale and mechanisms in the CCAF to protect data security. CCAF is demonstrated by the organization strategy based on the necessities and the employment established by the CCAF multi-layered security; when the work deals multi layers the efficiency degrade to overcome this problem.

3. Literature Survey

This study presented an overview of Mobile Cloud Computing (MCC), and identified the dimensions of the heterogeneity in MCC. MCC was more heterogeneous domain while compared to cloud computing due to the divergent computing paradigms and the networking technologies. The taxonomy of the heterogeneity roots was also devised. The pivotal roots of the heterogeneity and related approaches were analyzed and classified. The heterogeneity of the cloud computing and mobile computing was categorized [6].

This study described that the security is a big problem for the development of cloud computing data security. The security infrastructure was required to safeguard web and cloud services. At the user level, one needs to perform the trust negotiation and reputation aggression over all users. At the application end, the security precautions in worm containment and the intrusion detection against the virus attacks were established. This research work introduced homomorphic encryption mechanism and proposed a cloud computing data security scheme. The PaaS and SaaS services, providers, and users were equally responsible for preserving data integrity It was concluded that presently, the fully homomorphic encryption scheme has highly computational problem and it required further improvement [7].

This work described cloud data security encompasses a broad range of security constraints from an end user and cloud provider perspective, where the end user will be primarily concerned with the provider's data security policy, where their data will be stored, and also who could access to the data. The cloud security was important because it was the biggest reason where the organizations fear the cloud. This study proposed symmetric cryptography which solved the issues and implemented cloud as an efficient technology for storing the customer's data [8].

This research work described how trust value is calculated based on credential attributes such as availability, reliability, turnaround time efficiency and data integrity. A novel trust management system called QoS model was proposed. The QoS trust model performed better than the conventional FIFO model and similar trust models. The trust was measured in terms of four attributes. There were some attributes such as Honesty, Return on Investments and Utilization of Resources. In order to evaluate the performance, the experiments in a real heterogeneous environment with the combination of MS platform, UNIX platform, and Linux platform were carried out [9].

This research described that the advances in ICT were foreseen to dramatically change the public safety networks with the penetration of IoT devices and utilization of the cloud. The security was a significant challenge in field missions where hundreds of devices were connected by sending sensitive data to and from responders, and potentially allowing some data to be offloaded to the cloud. This study proposes the cloud centric multi-level authentication as a service approach for the responder devices. The main aim of this research work was to design a cloud centric public safety network which was not only resilient but also reliable. Such network was a cyber physical system that required seamless integration of the cyber and physical elements. The security and privacy have to be built when a public and reliable network was developed [10].

This research work demonstrated the CCAF multi-layered security for the data security in the Data Center under the proposal and recommendation of CCAF guidelines. The rationale, overview, components in the CCAF, where the design was based on requirements and the implementation was illustrated by its multi-layered security. This study explained how multi-layered security was a suitable method and recommendation, since it presented multiple protections and improvement of security for 10 PB of data in the Data Center based at the University of London Computing Center (ULCC) [11].

This study investigated the need of power consumption and energy efficiency in cloud computing model. It was shown that there were few major components of cloud architecture which were responsible for high amount of power dissipation in cloud. The possible ways to meet each sector for designing an energy efficiency model has also been studied [12].

4. Objective of the Proposed Research

To accomplish the aforesaid aim, the study has following objectives:

1. To address the present challenges of data access and data safety in cloud computing system.
2. To conduct a survey on several adoptive techniques for safe data recovery systems in cloud computing.
3. To develop a proposed technique which includes cloud computing adoption framework for effective data safety estimation in cloud computing.

5. Methodology of the Proposed Research

The data security and effectiveness estimation in cloud computing can be achieved by deployment of cloud computing Adoption framework. The steps to be followed in the safe data access in cloud computing system are given as follows.

Step 1: Initially, the input data will be fed to the cloud server.

Step 2: In the cloud server, according to the data sufficiency the datawill be compressed.

Step 3: The compressed data will undergo wavelet transformation. In wavelet transformation, the noise will be reduced and the key generation for each of the compressed data will be done.

Step 4: After the wavelet transformation is executed, the Advanced Encryption Standard (AES) is deployed for encrypting the data.

Step 5: After the encryption process, the Dragonfly algorithm is used to establish the key generation for all the compressed data. The AES and the Dragonfly algorithm are used to ensure the improved data storage.

Step 6: In cloudlet, the data are saved as folder wise in which the original data can be retrieved by means of the generated keys.

The block diagram of the proposed research methodology is shown below in Figure 1.

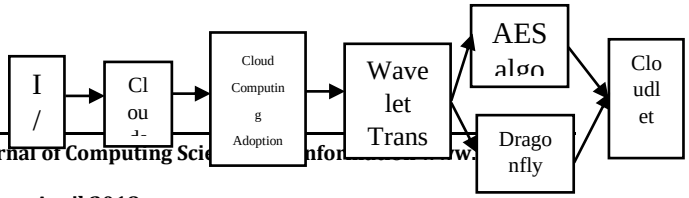

Figure 1: Block Diagram of the research method

Wavelet Transformation

The wavelet transform method includes de-noising approach which accounts that the wavelet coefficients corresponding to the signal contains important information of the signal, and they are of small number with small amplitude. The wavelet coefficients that correspond to the noise will be uniformly distributed. The wavelet transform can be divided into two types namely, soft threshold and hard threshold. The hard threshold method is to set a value of 0 for the wavelet coefficients that were smaller than the set threshold value. Those values which were greater than the threshold values were retained without any treatment. The soft threshold method also sets a value of 0 for the wavelet coefficients that were smaller than the set threshold value, but the values of the wavelet coefficients that were greater than the threshold value were set to the new shrunken values obtained by subtracting the threshold value from their original values [13].

The formula for the hard threshold is given as:

$$\lambda_{hard} = \begin{cases} x(t) & |x(t)| > \lambda \\ 0 & |x(t)| \leq \lambda \end{cases}$$

The formula for the soft threshold is given as:

$$\lambda_{soft} = \begin{cases} (|x(t)| - \lambda)\operatorname{sgn} x(t) & |x(t)| > \lambda \\ 0 & |x(t)| \leq \lambda \end{cases}$$

Where,

$x(t)$ is the signal wavelet transfer function

λ is selected threshold

sgn is the sign function

Advanced Encryption Standard (AES) Algorithm

AES is the most frequently used algorithm preferred for encryption. It is based on several substitutions, permutations and linear transformations, and each are executed on the data blocks of 16 bytes. AES algorithm is highly preferred because there is no attack against AES algorithm exists. Hence the AES algorithm remains as the preferred encryption standard for government sectors, banks and places where high security systems are required around the world [14].

Initially the plain text of 128 bits of block cipher will be the input. This will be treated as 16 bytes. Then each of the bytes will be integrated with a block of the round key using bit wise XOR. From S-Box the 16 input bytes will be exchanged resulting 4x4 matrices. Each row of this matrix will be shifted to the left. The shifting will be executed as follows.

i) First row will not be shifted.
ii) Second row will be shifted to one position to its left
iii) Third row will be shifted to two positions to its left
iv) Fourth row will be shifted to three positions to its left

As a result of these new matrices will be produced that contains same 6 bytes but it will be shifted with respect to each other.

Dragonfly Algorithm

The DA, being a meta-heuristic algorithm with better exploration and exploitation characteristics, is a suitable applicant for finding optimal solution. The several operations performed for exploration and exploitation of the DA such as separation, alignment, cohesion, attraction towards food source, distraction towards enemy concept is described [15]. The AES and dragonfly algorithm are used for the betterment of the data storage in cloud computing. In AES, in order to generate optimal keys, DA algorithm is used.

6. Proposed Outcome of this Research

The expected efficiency and outcome of the proposed research work can be formulated by several performance evaluations given as follows.

- Efficiency
- Throughput
- Constant Error Rate
- Bit Error Rate
- Data Transfer Rate

7. Conclusion

Cloud computing and its applications have a greater impact on several platforms such as industries, educational institutes, business, etc. The data storage and data access in cloud computing system in a safer way still remains as a challenge. Numerous research works have been done in cloud computing domain which evaluated several issues such as cloud data storage, security problem, privacy in data access, etc. This research work aims at ensuring data safety in cloud system and estimation of effectiveness by deploying Cloud Computing Adoption Framework. The input data fed to the client server. In cloud system, by using Cloud Computing Adoption Framework the data will be compressed and the data storage system will be enhanced by using Optimization techniques such as Dragonfly algorithm. The data after undergoing wavelet transform will be secured by generating key. The dragonfly algorithm to establish the key generation for all the compressed data. The AES and the Dragonfly algorithm are used to ensure the improved data storage. The compressed data can be retrieved by using the generated key.

8. References

[1] Ryan, M. D. (2011). Cloud computing privacy concerns on our doorstep. *Communications of the ACM*, *54*(1), 36-38.

[2] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, *500*(2011), 292.

[3] De Filippi, P., & Belli, L. (2012). The Law of the Cloud v the Law of the Land: Challenges and Opportunities for Innovation.

[4] Weinman, J. (2012). *Cloudonomics: The business value of cloud computing*. John Wiley & Sons.

[5] Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing. *IEEE Communications Surveys and Tutorials*, 1-15.

[6] Sanaei, Z., Abolfazli, S., Gani, A., & Buyya, R. (2014). Heterogeneity in mobile cloud computing: taxonomy and open challenges. *IEEE Communications Surveys & Tutorials*, *16*(1), 369-392.

[7] Zhao, F., Li, C., & Liu, C. F. (2014, February). A cloud computing security solution based on fully homomorphic encryption. In *Advanced Communication Technology (ICACT), 2014 16th International Conference on* (pp. 485-488). IEEE.

[8] Sugumaran, M., Murugan, B. B., & Kamalraj, D. (2014, February). An architecture for data security in cloud computing. In *Computing and Communication Technologies (WCCCT), 2014 World Congress on* (pp. 252-255). IEEE.

[9] Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, *233*(1), 281-292.

[10] Butun, I., Erol-Kantarci, M., Kantarci, B., & Song, H. (2016). Cloud-centric multi-level authentication as a service for secure public safety device networks. *IEEE Communications Magazine*, *54*(4), 47-53.

[11] Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*, *9*(1), 138-151.

[12] Banerjee, A., Agrawal, P., & Iyengar, N. C. S. (2013). Energy Efficiency Model for Cloud Computing. *International Journal of Energy, Information and Communications*, *3*(6), 29-42.

[13] Zhu, J., Xue, Y., Zhang, N., Li, Z., Tao, Y., & Qiu, D. (2017, April). A noise reduction method for Ground Penetrating Radar signal based on wavelet transform and application in tunnel lining. In *IOP Conference Series: Earth and Environmental Science* (Vol. 61, No. 1, p. 012088). IOP Publishing.

[14] Pancholi, V. R., & Patel, B. P. (2016). Enhancement of cloud computing security with secure data storage using AES. *International Journal for Innovative Research in Science & Technology*, *2*(09).

[15] Mirjalili, S. (2016). Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. *Neural Computing and Applications*, *27*(4), 1053-1073.