Green Cloud Computing Ideas with Security Issues in Setting of Distributed Computing and Cloud Framework

Fitria, Suhendro Yusuf, SeptiliaArfida, HendraKurniawan

Faculty of Computer Science, Darmajaya Institute of Business and Informatics, Lampung, Indonesia.

Abstract— *Cloud is a popular paradigm with extreme abilities and benefits for trending ICT environment. On the other end the major concern came in terms of security and privacy while adopting the cloud technology. This has brought about another examination pattern on the security issues of cloud. As cloud administrations are free of natural scattering, impressible data of various substances is ordinarily put away in remote servers and areas. This has huge potential outcomes of being presented to undesirable parties. In the event that security is not blasting and trustworthy, the consistence and in addition to indicates that cloud computing has offer will lose its viability. This paper illuminates the cloud computing ideas with security issues in setting of distributed computing and cloud framework.*

Keywords— *green cloud computing, security, distributed computing, cloud framework*

I. Introduction

In today's World, Cloud Computing is gaining highest popularity as one of the most creative technological approach that has revolutionized the way of computing [1]. Cloud computing has Internet as its ground which provides the user a foundation of shared computer processing resources instead of buying all the hardware/software [2].Initially, storage was a big issue for users as they had to explicate on high storage discs for large data. But with the introduction of Cloud Computing technology, a major solution to this problem was found as now it became quite easy to store and access their data that may be located anywhere in the world.In simple terms, it means that instead of buying all the resources, one can easily rent some computational power, storage, databases and any other resource just by paying some minimal charges depending upon the provider's service charges [3]. Cloud Computing is booming among business, user and enterprises because it has made investments smaller and oriented to operations rather than to assets acquisition.Cloud is a popular paradigm with extreme abilities and benefits for trending ICT environment. On the other end the major concern came in terms of security and privacy while adopting the cloud technology. This article is an effort to cover the

challenges in fields like storage, virtualization and communication in cloud [4].Also it is a try to elaborate relevance of current cryptographic approach in order to increase security of cloud in ICT, through which they can store and process their information in a third party data center whose distance from the user's range may vary from across a town to across a continent. Cloud computing depends on mutual pooling of resources to accomplish integrity and economy of scale [5]. Figure 1 shows Cloud Computing.

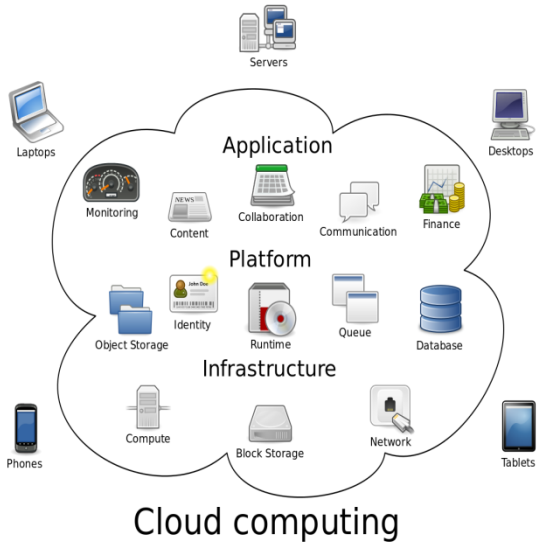

Figure 1. Cloud Computing

Cloud computing is emerging as a new world of possibilities ,it is a demand based service model which provides elasticity in resource management whose resources get shared and pooled to be used by multiple users [6]. Simultaneously privacy and security issues are major concern in cloud computing. Normally in cloud computing resources like data and application are hosted on cloud service providers (CSP) on controlled locations where customers have less privileges over them. This paper covers few security problems of cloud computing technology, have analyzed the importance of cryptographic methods while facing their issues [7].

The administration models are as per the following:

a) Cloud Software as a Service (SaaS)—Use supplier's applications over a system.
b) Cloud Platform as a Service (PaaS) —Deploy client made applications to a cloud.
c) Cloud Infrastructure as a Service (IaaS) —Rent handling, stockpiling, organize limit, and other basic registering assets.

The deployment models, which can be either inside or remotely actualized, are abridged in the NISTintroduction as pursues:

1) Private cloud—Enterprise claimed or rented.
2) Community cloud—Shared foundation for explicit network.
3) Public cloud—Sold to general society, super scale foundation.
4) Hybrid cloud—Composition of at least two mists.

II. Evolution of Cloud Computing

One day in a talk at MIT around in 1960 John McCarthy demonstrated that like water and power, preparing can in like manner be sold like an utility. Additionally, in 1999, the Salesforce Company started passing on the applications to the customers through a beneficial site. Amazon Web Services were started by Amazon in 2002 and they were giving the organizations of limit and computation. In around 2009 noteworthy associations like Google, Microsoft, HP, Oracle had started to give conveyed registering organizations [8]. These days every single individual is utilizing the administrations of distributed computing in their day by day life. For instance Google Photos, Google Drive, and iCloud and so on [9]. In future distributed computing will turn into the fundamental need of IT Industries. Figure 2 shows evolution of cloud computing.

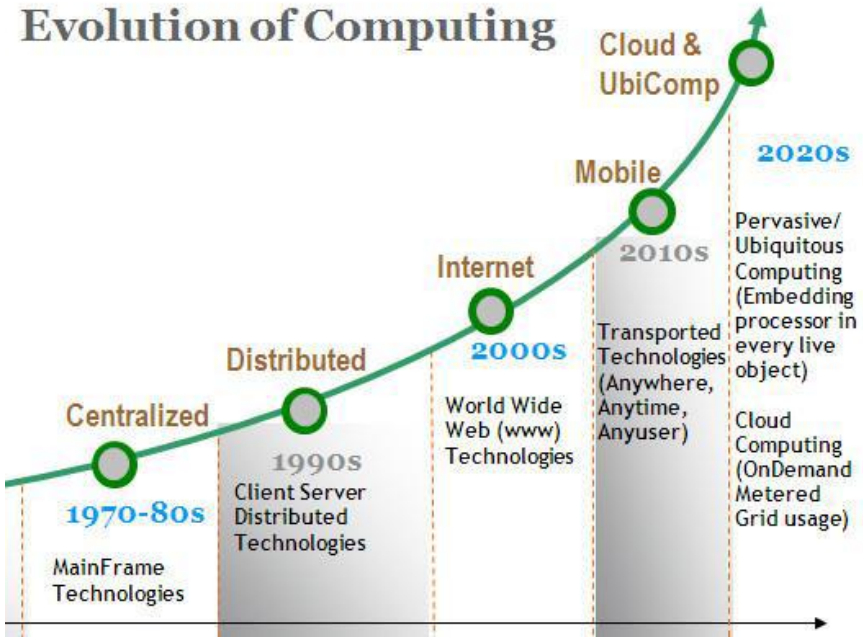

Figure 2.Evolution of Cloud Computing

III. Working of Cloud Computing

The cloud is basically divided into two major layers. These are the back end layers and the front end layers.The layers through which user interacts are the front layers. Considering an example of facebook, when you access your profile, you are actually viewing that software that is running on front end [10].Likewise, the back end comprises both the hardware and the softwarearchitecturethatdeliversthedatawithwhicha normal user interacts.Clouds use a network layer to connect user to the resources which are consolidated in the data center. Users use devices like Tablets, computers and mobile phones to connect with center. The way of accessing the data center is divided mainly via a company network or the internet or both [11]. One of the major benefits of cloud is that it can be accessed from any location which helps mobile workers to access their business systems on demand. Figure 3 shows working of cloud computing.

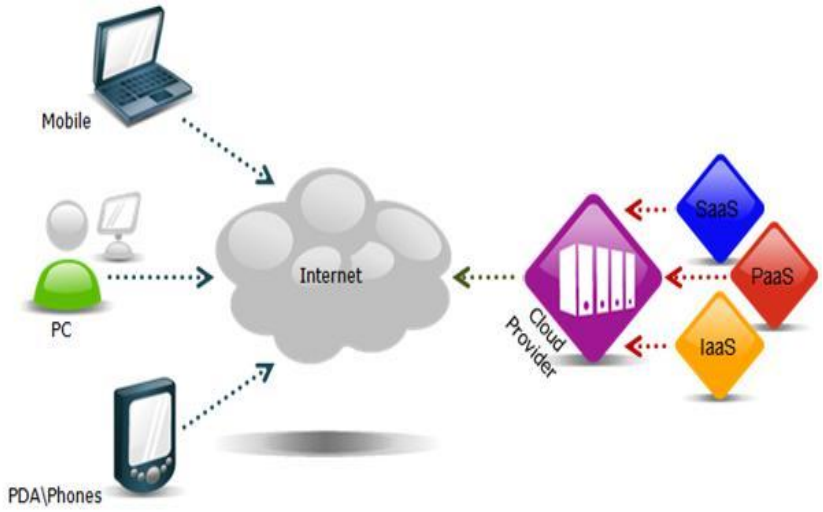

Figure 3. Working of cloud computing

All the applications which are executed on cloud enjoy the affability of the computing power. All are made to execute simultaneously which indicates as if all apps are running on one separate machine.This opens up the doors for the users to usewhatever amount of resources theywant to use irrespective of space and capacity. Also, it kills the practice of assigning any particular hardware system for that particular job in advance [12].Cloud Computing makes heavy lifting a lot easier. It works on the concept of workload shift. Now, the local computers no longer need to do the heavy lifting for the proper functioning of applications installed. It is well handled and executed by the web of networks that are responsible for construction of the cloud.The only thing which has to be taken care by the user is the proper interaction with the computing systems interface software [13].

E.g. Handling the Web Browser or login into your account etc and the rest is automatically taken care by the networks.

IV. Advantages of Cloud Computing

Cloud computing is an IT model or figuring condition made out of IT segments (equipment, programming, systems administration, and administrations) just as the procedures around the sending of these components that together empower us to create and convey cloud administrations by means of the Internet or a private system [14]. The generating and cancellation of virtual machines running on physical equipment and being constrained by hypervisors is a cost-proficient and adaptable figuring worldview.

Following are the key highlights of distributed computing:

1. Resource Pooling and Elasticity
2. Self-Service and On-Demand Services
3. Pricing
4. Quality of Service

Cloud computing is booming now a days due to the following advantages [15]

A. Flexibility

Cloud-basedassistanceisexcellentforbusinessesthat have increasing or changing bandwidth requirements. If your demand grows it's effortless to add up your cloud capacity, similarly, if you can scale down again according to your need.

B. Disaster Recovery

Business do huge investment for disaster recovery but this is not possible for the small business as it requires money and maintenance. Cloud computing saves time through it cloud- based backup and recovery services as it reduces the large investments and add third party expertise into the deal.

C. Automatic Software Updates

Cloud computing servers are far located and these are regularly updated and maintained by the suppliers and hence there is a reduction of burden on the companies and gives them opportunity to focus on their business rather than other unnecessary aspect.

D. Capital Expenditure Free

Cloud computing reduces the high investment done on hardware and infrastructure. Company just has to pay according to their usage and can change the scale of their usage according to their

demand. Hence there is no wastage that existed when hardware was left idle due to lower demand.

E. Increased collaboration

The user can access, edit and share the data irrespective of the time and the location. This increases the productivity as cloud based workflow and file sharing aids in making up gradations quick and easy.

F. Work From Anywhere

All cloud computing requires is an internet connection. Hence a user can work on cloud irrespective of the device that he is using as the data is centrally located in the data centers and not on the device making it easy and comfortable for the user .

V. General Challenges in Cloud Security

Basically we can divide a cloud security in three main levels as shown in Figure 4.

1. Storage Level
2. Communication Level
3. Virtualization Level

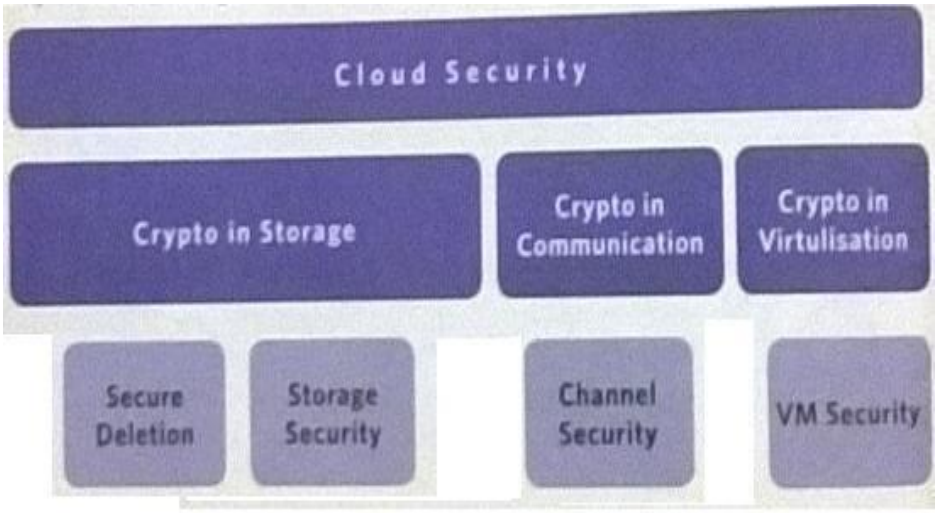

Figure4. Cloud Security

Now we can discuss the uses of cryptography at these levels in a sequential manner.

(1) Cryptography at storage Level:- Almost an infinite no of onlineservicesareusingthecloudstorageforarchiving backup of data as well as primary storage.

And an efficient system will hide the storage related complexities and must provides a simple online interface.

Here two major areas are covered at this level.

(i) Secured data storage:-Stored data in cloud should be so secured that only authorized and authenticated user can only access and process and process this data.If a data is hosted in-house an efficient authentication system may be good enough to protect it. But in cloud due to limited visibility of control implementation a user/customer feels insecured about its data storedoncloud.

ACSPmustmaintainahigherlevelof security using various methods. One way could be the encryption of data to ensure security. However the encryption is not so practical for data at rest in some cases like s/w as a service (SaaS) & platform as a service(PaaP) models, because it is almost impossible to perform some operations like searching and indexing, if data is encrypted. In the PaaS,Platformspecifieslogsaremaintainedbuttheyget shared in separate log stores of cloud [16]

As we know that logs may carry a sensitive information and requires a protective cryptographiccontrolstomaintainconfidentialityand integrity.SowecansaythatinPaaS&SaaSmodels encryption is not so useful, whereas it is better to use encryption at data storage at rest,data in transmission and various log files. Another category infrastructure as a service (IaaS) where storage is provided as a service it is desired tohave encryption which is feasible for security of data. Here normally storages are scattered across various geographic locations along with multiple copies of data achieve high availability requirements in cloud [17].

Here transmission of data between these storage nodes must be secured as the data moves over public networks which is vulnerable to compromises [18].

(ii)Secureddeletionofdataincloud:-Afterdeletionof data,it must not be available in future within the cloud. This deletion of data may be due to various reasons:-

1)Expiry of contract period

2)Migration to another CSP

3)Routine deletion of data which is of no use.

Practically it is challenging for customers to clean out the data completely after using cloud services, as the physical storage devices of data are not directly accessible to the customers. Actually cloud follows alayeredstoragesystem andeach layer may cache the data and its traces. To make sure the availability of data it is also possible that same data stored at multiple locations without data owner knowledge which leads to the situation that the data copy is stored even after

expiry of contract and the customer has no option to control it and track such copy operation [19].

Even after deletion of data from all locations still this is a possibility of leftover of data because simple delete operation may delete the link only to the data instead of actual data from storage devices. Sowecan'tdeny that theremaining data could not be used someone else with any malafied intentions. Though some IT giants like Google started deletion of user data by including (Inactive account settings) but such options are controlled by CSP itself only [20].

Now the option is a direct way of deletion of data by providing access to data files to its correct owner but it is quite impractical in a multi-location environment and need a very honest and strong assumption that the concerned CSP will definitely provide the access to all storage devices, where the data has copied while using the cloud services.

So we can't consider this way also feasible. Another option is the use of cryptography again whereencryption of data and management of keys is needed. The dataneedstobeencryptedfirstandthenstoredincloud storage in this way if a key is delete locally permanently the data may remains available physically but of no use as it is encrypted and cannot retrieved back without the key. Such data is almost equal to deleted data. Some researchers have proposed this method based on policy controls. Though it is quite better than others methods of data deletion but still it needs a highly efficient cryptographic operations.

(2) Cryptography in communication

Transfer ofdatabetweenCSPandcustomerorwithin component of cloud setup happens in cloud computing. This requiresasecurecommunicationsignificantlywithouta secured communication channel no cloud environment can be claimed secured for web services. Public network are used by thecloudservicesthatisconsideredunnecessarywithout additional security provisions. Virtual privatenetwork (VPN) and secure socket layer(SSL) encryption are widely used as a solution to counter and decrease the risk of data. Compromisationoveranetworkinacloudenvironment. Therefore cryptographic methods here also plays a crucial role in protection of data while its transfer.

(3) Cryptography in virtualization

Virtualization is a common phenomenon widely used in computing. In cloud environment virtualization exists. Here virtual machines exist which share a common physical resources but have complete logical isolation. So availability and integrity are two critical issues which might affected by visualized cloud environment may expose a VM to dangerous side channel attack which may leads to leakage of sensitive data.

Here again the cryptographic protocols may plays an important. Operations like hashing and message authentication code also ensure the detection of breach of VM's integrity. Encryption of

sensitive files placed on virtual disk along with proper access control also prevents chances of malicious code injection inthedisk.Virtual trustedplatform management (VTPM) is also an approach proposed by IBM researchers to create a protective storage and cryptographic coprocessor for a secured h/w environment.

VI.Conclusion

The same number of organizations move their information to the cloud the information experiences numerous progressions and there are numerous difficulties to defeat as business applications must be re-planned in an unexpected way. The aftereffect of this is information security nearly quits being the essential concern. Accomplishing the necessities for cloud information security involves applying existing security systems and following sound security rehearses. To be powerful, cloud information security relies upon more than basically applying suitable information security methods and countermeasures. Here again the cryptographic protocols may plays an important. Operations like hashing and message authentication code also ensure the detection of breach of VM's integrity. Encryption of sensitive files placed on virtual disk along with proper access control also prevents chances of malicious code injection in the disk. Virtual trusted platform management (VTPM) is also an approach proposed by IBM researchers to create a protective storage and cryptographic coprocessor for a secured h/w environment.

References

[1]. Jeba, J. A., Roy, S., Rashid, M. O., Atik, S. T., &Whaiduzzaman, M. (2019). Towards green cloud computing an algorithmic approach for energy minimization in cloud data centers. International Journal of Cloud Applications and Computing (IJCAC), 9(1), 59-81.

[2]. Masdari, M., &Zangakani, M. (2019). Green cloud computing using proactive virtual machine placement: challenges and issues. Journal of Grid Computing, 1-33.

[3]. Alarifi, A., Dubey, K., Amoon, M., Altameem, T., Abd El-Samie, F. E., Altameem, A., ...& Nasr, A. A. (2020). Energy-Efficient Hybrid Framework for Green Cloud Computing. IEEE Access, 8, 115356-115369.

[4]. Ismail, A. H., El-Bahnasawy, N. A., &Hamed, H. F. (2019). AGCM: active queue management-based green cloud model for mobile edge computing. Wireless Personal Communications, 105(3), 765-785.

[5]. *Patil, A., &Patil, D. (2019, February). An Analysis Report on Green Cloud Computing Current Trends and Future Research Challenges. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.*

[6]. *Jangiti, S., Ram, E. S., &Sriram, V. S. (2019). Aggregated Rank in First-Fit-Decreasing for Green Cloud Computing. In Cognitive Informatics and Soft Computing (pp. 545-555). Springer, Singapore.*

[7]. *Kaushal, S., Gogia, D., & Kumar, B. (2019). Recent trends in green cloud computing. In Proceedings of 2nd International Conference on Communication, Computing and Networking (pp. 947-956). Springer, Singapore.*

[8]. *Singh, A., Sinha, U., & Sharma, D. K. (2020). Cloud-Based IoT Architecture in Green Buildings. In Green Building Management and Smart Automation (pp. 164-183). IGI Global.*

[9]. *Lu, Y., & Sun, N. (2019). An effective task scheduling algorithm based on dynamic energy management and efficient resource utilization in green cloud computing environment. Cluster Computing, 22(1), 513-520.*

[10]. *Jangiti, S., Subramaniyaswamy, V., & Shankar, V. S. (2019). Bulk-bin-packing based migration management of reserved virtual machine requests for green cloud computing. EAI Endorsed Transactions on Energy Web, 6(24).*

[11]. *Bhavani, M. R., Begum, M. J., &Krupamai, Y. S. A COMPREHENSIVE ANALYSIS ON INDUSTRIAL NETWORKING CYBERSECURITY ISSUES BASED ON LI-FI WITH GREEN CLOUD COMPUTING.*

[12]. *Aslam, A. M., &Kalra, M. (2019). Using Artificial Neural Network for VM Consolidation Approach to Enhance Energy Efficiency in Green Cloud. In Advances in Data and Information Sciences (pp. 139-154). Springer, Singapore.*

[13]. *Bhattacherjee, S., Das, R., Khatua, S., & Roy, S. (2019). Energy-efficient migration techniques for cloud environment: a step toward green computing. The Journal of Supercomputing, 1-29.*

[14]. *Zhou, Q., Xu, M., Gill, S. S., Gao, C., Tian, W., Xu, C., &Buyya, R. (2020). Energy efficient algorithms based on VM consolidation for cloud computing: comparisons and evaluations. arXiv preprint arXiv:2002.04860.*

[15]. Iqbal, M. A., Aleem, M., Ibrahim, M., Anwar, S., & Islam, M. A. (2019). Amazon cloud computing platform EC2 and VANET simulations. International Journal of Ad Hoc and Ubiquitous Computing, 30(3), 127-136.

[16]. Suresh Kumar, D., &JagadeeshKannan, R. (2020). Reinforcement learning-based controller for adaptive workflow scheduling in multi-tenant cloud computing. The International Journal of Electrical Engineering & Education, 0020720919894199.

[17]. Singh, S., Ra, I. H., Meng, W., Kaur, M., & Cho, G. H. (2019). SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. International Journal of Distributed Sensor Networks, 15(4), 1550147719844159.

[18]. Maseleno, A., Huda, M., Jasmi, K. A., Basiron, B., Mustari, I., Don, A. G., & bin Ahmad, R. (2019). Hau-Kashyap approach for student's level of expertise.Egyptian Informatics Journal, 20(1), 27-32.

[19]. Galán, S. G., Seddiki, M., de Prado, R. J. P., Expósito, E. M., Marchewka, A., & Reyes, N. R. (2020, July). Relevance of Using Interpretability Indexes for the Design of Schedulers in Cloud Computing Systems. In 2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE) (pp. 1-8). IEEE.

[20]. Kumar, M., Sharma, S. C., Goel, A., & Singh, S. P. (2019). A comprehensive survey for scheduling techniques in cloud computing. Journal of Network and Computer Applications, 143, 1-33.