Cost Efficient Media Cloud Storage and Systematic Risks Involved in the Cloud Computing

Arif Ali Wani, Aamir Khan, Gaurav, Ahmad Jamal and Piyush Kumar Gupta

Abstract*: Now a days data is growing at a very fast rate. Here data is referred not only with organizational data but the data also from non-organizational and social media, the data may be PDF's, Photos, Audios, Videos, XML file etc. To earn more profit, the organizations tends to establish Cloud Storage with minimum establishment cost and high security. To provide robust and secure platform is the main aspect of cloud. Lots of algorithms have been designed and implementing for securing the data at cloud but the attack on 2014 on cloud in which 50 million accounts were hacked, shows that cloud is not fully secured. The main focus of this paper is to draw attention towards security issues and cost-efficient cloud and the solution for implementing it.

***Index Terms*: Inter-cloud Computing, Cost efficiency, Overload, System risks.**

I. INTRODUCTION

With the advancement of Globalization data is incremented exponentially. In order to arrange this data, the companies providing clouds can rent their technologies to users and earn profit. Client typically pay service fee monthly or annually [1]. Clients who subscribe to cloud computing can achieve a variety of benefits depending on their particular need. Building a distributed cloud system with surplus resources requires lots of money and have risks of stolen of data.

In this context, this paper proposes:

(i) C-CLOUD, a cost-efficient democratic cloud infrastructure made of dynamically and temporarily shared surplus computing resources.
(ii) Inter cloud and media cloud communication.
(iii) Security issues in cloud computing.
(iv) Security of cloud

II. C-CLOUD: SYSTEM OVERVIEW

Figure 1 shows the working and architecture of C-CLOUD. In particular, C-CLOUD generates a cloud from resources Which are not part of any cloud infrastructure. Clients typically pay service fee monthly or annually[2]. Clients who subscribe to C-CLOUD can achieve a variety of benefits depending on their particular need and get revenue in return from the C-CLOUD[3]. Figure 1 further shows a high-level functional architecture of C-CLOUD. Primarily, C-CLOUD takes reservation requests as inputs and allocates the requests to the dynamically shared resources. Thus, it is important to provide proper incentives to the clients of C_CLOUD such that the cost of serving the requests is low[4].

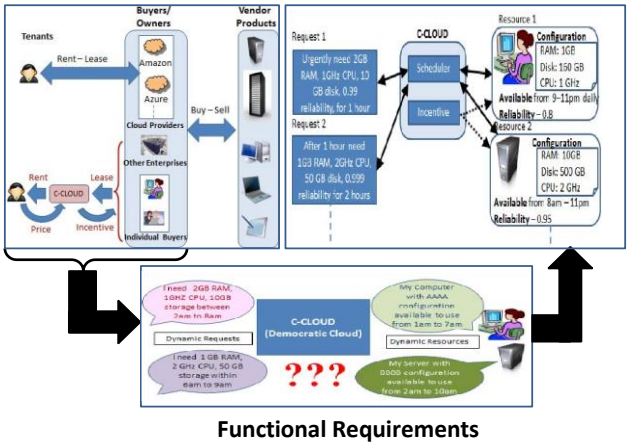

Fig 1: Vision, requirements, and high-level architecture of C-CLOUD.

III. INTER CLOUD AND MEDIA CLOUD COMMUNICATION

Communication of two or more clouds with each other is known as Inter-Cloud Communication and when there are multiple clouds involved in a scenario, they communicate with each other internally creating inter cloud computing[5]. This is also important to meet the increasing demands as diverse type of requirements can be made by the user, which may not be offered by one single cloud. In order to encounter the requisite, one has to request either multiple or another cloud. Other than this, cloud should be able to discover services available elsewhere. This inter-cloud computing will create a 'Cloud of Clouds' (CoC), being able to communicate the data that is not stored by its datacenters directly[6].

Revised Manuscript Received on July 06, 2019.

Arif Ali Wani, Computer Science and Engineering Department, Glocal University, Saharanpur, India.
Aamir Khan, Computer Science and Engineering Department, Uttarakhand Technical University, Dehradun, India.
Gaurav, Department of CSE, SEST Jamia Hamdard, New Delhi – 110062, India.
Ahmad Jamal, Computer Science and Engineering Department, Glocal University, Saharanpur, India.
Piyush Kumar Gupta, Department of CSE, SEST Jamia Hamdard, New Delhi – 110062, India.

A. Inter Cloud Communication Entities

Inter cloud computing involves four entities as listed below.

i. Cloud Service Provider

Cloud service provider is the organization which provide services to the Cloud Customers, Cloud Service Partner and other Cloud Service Providers[7]. These typically include Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS).

ii. Cloud Service Customer

Cloud Service Customer is the person which uses Cloud Services and has a relationship with Cloud Service Provider.

iii. Cloud Service Partner

Cloud Service Partner works as a bridge between Cloud Service Provider and Cloud Service Partner. Cloud Service Partner is a third party which has a role of Cloud Auditor, Cloud Developer and Cloud Broker. Cloud Auditor, audits the Cloud and provides quality services. Cloud Developer develops the Cloud to provide services to the Cloud Customers at a low cost and reduce risks of cyber attacking[8]. Cloud Broker deals with the business aspects and try to sell the Cloud to Cloud Customers and other Cloud developers.

iv. Cloud Service Carrier

Cloud Service Carrier acts as an interference between Cloud Service Providers and Cloud Customers just how channel works in between Sender and Receiver. It transports the Cloud Services from Cloud Provider to Cloud Customers through networks and other web services.

Data is timeliness means that data is kept for years but whenever data is retrieved it should be quick[9].

IV. SECURITY ISSUES IN CLOUD COMPUTING

A. Abuse and nefarious use of cloud computing

A large processing capability as well as unlimited storage capacity can be provided to their users. Some cloud providers offer a period of essay for free. So, by exploiting these high performances and processing capacity provided by the cloud, hackers and malicious people can use it to crack cryptographic keys that are very difficult to break on a simple computer. One more case can be a hacker can exploit the cloud servers performance simply by performing DDOS attacks also by sharing malicious softwares and harmful virus[10].

B. Malicious Insiders

Another threat to Cloud Computing is the malicious insiders. Malicious insider is considered as a common threat to all organizations. A malicious hacker can be an old employee, a recipient or a business partner who succeeds to have access to the system or data for malicious purpose[11]. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees.

C. Data Loss or Leakage

The data in the Cloud are very loosely tied as in terms of Data Migration and Security. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment[6].

D. Account or Service Hijacking

Hijacking is a type of network security attack in which the attacker takes control of a communication. Attack method such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Because of this vulnerability if an attacker succeeds in obtaining access to user credentials, he can access critical areas of data services in cloud environment, he also can spy on users activities and operations[8].

V. SECURITY OF CLOUD

Cloud computing security refers to the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment[12]. The security of Cloud computing addresses logical as well as physical issues over the various different infrastructures, softwares and platforms. It also addresses how these services are delivered (public, private or hybrid delivery model). Security allows the confidentiality, integrity, authenticity and availability of information. The development of technologies and their standardization makes available a set of algorithms and protocols for responding to these issues[13].

A. Asymmetric Encryptions

This cryptographic technique uses two separate keys, out of which one is public which is used to encrypt plain text and the other is private which is used to decrypt the encrypted cipher text. A pair of keys is generated and one of them is nominated as the Public Key and is published. Any parties wishing to communicate securely with the key's owner encrypt the message using the recipient's Public Key. The decryption can only be accomplished by knowing the second, Private, key, which the owner ensures is never released[14]. RSA cryptographic algorithm uses two different keys one is Public Key which is used by everyone and the other is Private Key which will be kept private to decrypt the text. The ideology of RSA algorithm is using two different keys of large integers as it is difficult to factorize large integers. It uses two numbers (let's say p and q) of 256 bits each and public key (let's say n) which is of 512 bits and contains the product of two large prime numbers p and q. So, N = P x Q which is Public key. Now the private key is also derived from these two prime numbers which we took for creating Public Key. Therefore if we see the above formula and calculate them we can conclude that the encryption strength totally lies on the key size and if we increase the key size by two times or three times the strength increases exponentially.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

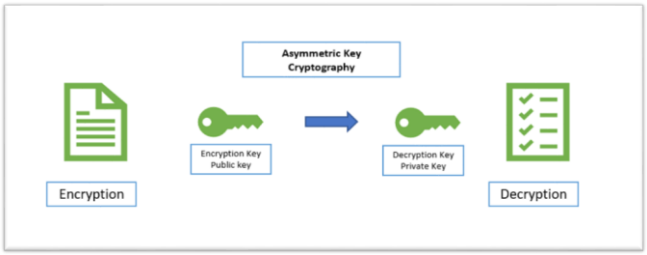

Figure 2: A systematic block diagram of Asymmetric key Cryptography.

B. Symmetric Encryptions

This cryptographic technique uses same cryptographic keys, which is used to encrypt plain text to cipher text and to decrypt the encrypted cipher text to plain text. Symmetric encryption is used to share information between a set of people that all shall have access to it. Furthermore, symmetric encryption is nice because it is easier to understand[11].

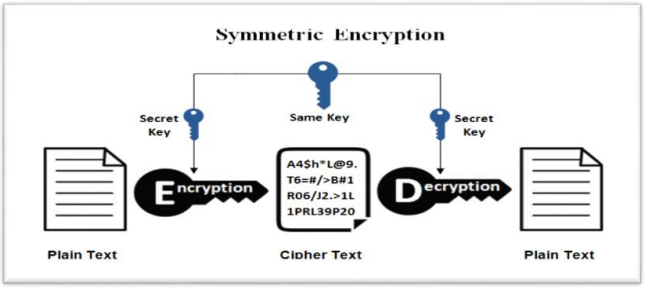

Figure 3: A systematic block diagram of Asymmetric key Cryptography.

The most common symmetric encryption algorithm is AES which has a fixed block size of 128 bits and different variants in key size as 128, 196, 256 bits.

AES is more secure than its predecessors -- DES and 3DES -- as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES, making it ideal for software applications, firmware and hardware that require either low latency or high throughput.

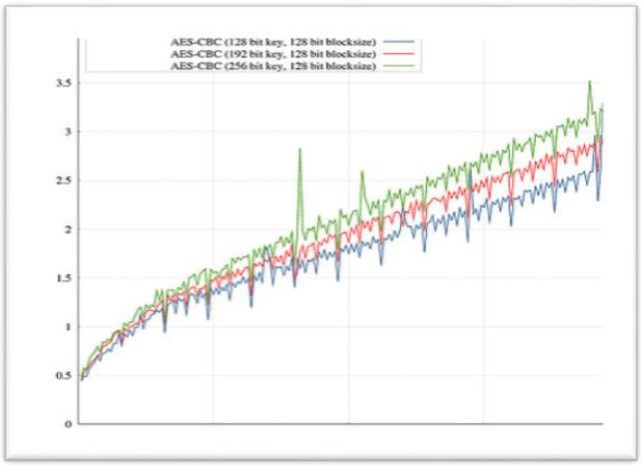

Figure 4: Speed of AES algorithm at 128, 196 and 258 key sizes.

VI. CONCLUSION

This paper introduced C-CLOUD, a cost-efficient reliable democratic cloud of surplus resources with the minimum risks involved in using it. To this effect, this paper proposed an incentive mechanism. The concepts of incentives for sharing resources and being aware of SLAs and task success probability make the proposed C-CLOUD unique to any other resource sharing paradigm, e.g. volunteer computing. C-CLOUD is further designed in a way that a user can get the flavor of modern-day cloud infrastructure-as-a-service; albeit hosted over a set of dynamically shared and potentially unreliable resources with guarantees on task completion success. Major issues in the deployment revolve around interactions between the CCLOUD and the resources shared for periodically checking the resource status (e.g. capability, reliability, availability, etc.). For handling these interactions, we use an existing open source distribution for volunteer computing.

REFRENCES

1. A. Hendre and K. P. Joshi, “A Semantic Approach to Cloud Security and Compliance,” 2015.
2. L. Krithikashree, S. Manisha, and M. Sujithra, “Audit Cloud : Ensuring Data Integrity for Mobile Devices in Cloud Storage .,” 2018 9th Int. Conf. Comput. Commun. Netw. Technol., pp. 1–5, 2018.
3. L. Logeswaran, H. M. N. D. Bandara, and H. S. Bhathiya, “Performance , Resource , and Cost Aware Resource Provisioning in the Cloud,” 2016.
4. V. Marbukh, “On Systemic Risk in the Cloud Computing Model,” 2014.
5. O. Wenge, D. Schuller, and R. Steinmetz, “Towards Establishing Security-Aware Cloud Markets,” 2014.
6. D. Zhe, W. Qinghong, S. U. Naizheng, and Z. Yuhan, “Study on Data Security Policy Based On Cloud Storage,” 2017 ieee 3rd Int. Conf. big data Secur. cloud (bigdatasecurity), ieee Int. Conf. high Perform. smart Comput. (hpsc), ieee Int. Conf. Intell. data Secur., pp. 145–149, 2017.
7. M. Joshi, K. P. Joshi, and T. Finin, “Attribute Based Encryption for Secure Access to Cloud Based EHR Systems,” 2018 IEEE 11th Int. Conf. Cloud Comput., pp. 932–935, 2018.
8. M. Carroll, A. Van Der Merwe, and P. Kotzé, “Secure Cloud Computing Benefits , Risks and Controls.”
9. A. C. Review, “Cloud Security Risk Management,” 2015.
10. K. Divya, “Key Technologies in Cloud Computing,” pp. 196–199.
11. B. L. R. Arif Ali Wani, “Discovery of knowledge by using Data warehousing as well as ETL processing,” Int. J. Recent Technol. Eng., p. 10, 2019.
12. A. A. Wani and B. L. Raina, “Issues and handy Solutions addressed at every stage in real time data warehousing , i . e . ETL (extraction , transformation & loading) - Literature Review,” no. X, pp. 1–5.
13. A. A. Wani, U. Chandra, and P. Jain, “International Journal of Research in Engineering and Innovation Performance analysis of FME based servers and cloud for data loading in big data and machine learning models for future data mining process , knowledge discovery in geo-spatial data,” vol. 1, no. 1, pp. 68–71, 2019.
14. A. A. Wani, U. Chandra, P. Bansi, and L. Raina, “Security Challenge in Big Data for Behaviour Analytics,” vol. 5, no. 7, pp. 578–581, 2018.

AUTHORS PROFILE

Arif Ali Wani received his Bachelor’s degree in Information and Technology from Model Institute of Engineering and Technology (MIET) affiliated to Jammu University, Jammu India. During the 2008 and M.Tech in Computer Science and Engineering from Gurgaon College of Engineering affiliated to Maharshi Dayanand University Rohtak, during the year 2013. Pursuing Ph.D. degree in Glocal University, Saharanpur Uttar Pradesh.

He is having 9 years of teaching experience, his area of business is Data Warehouse and Data mining, Computer Network. He has published and presented Research papers in journals, international and national level conferences.

Aamir Khan received his Bachelor's degree in computer application Uttaranchal institute of management Dehradun uttarakhand affiliated to HNBGU (central university), India. During the 2008 and master degree(MCA) Computer Science and Engineering from GB pant engineering college ,pauri During 2014.He has SET(State Eligibility Test) Qualified in year 2017and Pursuing Ph.D. Degree in Uttarakhand Technical University (State Govt. University) Dehradun. He is having 4 years of teaching experience; his area of business is Data Mining and big data analytics, Computer Network, Web technologies. He has published and presented Research papers in journals, international and national level conferences.

Gaurav has completed his M.Tech in Software Engineering from University Institute of Engineering & Technology, Maharshi Dayanand University, Rohtak (Haryana) in the year 2011. He received his B.Tech in Computer Engineering from University Institute of Engineering & Technology, Maharshi Dayanand University, Rohtak (Haryana) in the year 2009. He is having 8 years of teaching experience. He has published his research in peer reviewed International Journals, Book Chapters, and Conferences. His research interest includes Steganography, Image Processing, cryptography etc.

Ahmad Jamal A software engineer in computer science by qualification, with 5-year experience of Development and Deployment and 3-year experience in the research area. Solutions-driven programmer and a researcher with a track record of commended performance in modular and object-oriented programming, Well-versed in all phases of the software development lifecycle, with a strong working knowledge of algorithms and data structures. He has a bachelor degree in the P.C.M. and master degree in computer science, He is also certified the Business Professional Programmer by NIELIT formerly Doeacc (Ministry Of HRD). He is doing his Ph.D. in the are of ERP and Knowledge Base creation from Glocal University. His area of interest is to write the business logic of the application. His work calendar also includes research about new technologies. He is the mentored CS students on various projects and technicalities.

Piyush Kumar Gupta has received his M.Tech drgree in Software Engineering from National Institute of Technology, Durgapur, West Bengal in the year 2014. He completed his MCA degree in Computer Application from Gautam Budhh Technical University (GBTU/Former UPTU) in the year 2010 and B.Sc. in Math and Physics in the year 2005. He is having 5 years of teaching experience. He has published his research in peer reviewed International Journals, Book Chapters, and Conferences. His area of research interest includes Steganography, Machine Learning and etc.