Security enhancement of Online Accounting Data from Cyber Attacks

S. Gopalsamy, AV. Karthick

Abstract**: *The growing use of digital technology among businesses has highlighted the significance and function of cybersecurity as a fresh dimension of risk management, not least because cyber threats and hazards have drawn considerable public attention. Users typically do not understand the precise place of their information or the other jointly recorded information sources with theirs. The exchange of data on cybersecurity lists a comprehensive list of prospective advantages for government and private sector organizations. Cloud Accounting (CA) plays a predominant role in corporate finance. CA is a type of lease based accounting services. Client access the accounting package anywhere in the world. The major issue in Accounting is to secure accounting data. The aim of this is to provide a deep understanding of security vulnerabilities and solutions in online accounting with specific reference to cloud accounting. The proposed efficient double secured accounting environment for business using bio-metric based Iris, Rivest Shamir Adleman (RSA) and Advanced Encryption Standard (AES) algorithms provides the double standard highest security for online accounting applications. The author designing a prototype model to solve the issues related to security in the cloud accounting problem, this model is used to tackle the intruders from data hijacking. The results suggested that the proposed system gives an enhanced security mechanism in terms of high privacy and confidentiality. The major contribution of the study is the use of protecting valuable data from intruders.***

Keywords : data; security; accounting; corporate finance; biometric; Iris; encryption; client.

I. INTRODUCTION

Cloud Accounting is also called an online accounting system. It utilizes the accounting software where both the software and the data stored online. Data is more precious for every business enterprise. There is a Service Level Agreement (SLA) between the client and CA Service Provider (CASP). CASP denotes [12] the use of the internet for recording the transaction and pricing. As there is a huge demand for CASP they tie up with another is called the federated cloud. It offers service in terms of pay per use. CA reduces the cost [21] of operation and acquisition was drastically increased. In the consumer-centric model [1] the client calculates the price for remotely used service. Accounting was one of the important components of business activity. This paper deals about the decision making [23] regard select the right accounting package to its enterprise. The traditional accounting system [15] fails to fulfill the security needs of client needs due to the structural design of the system. It helps the business [8] to forecast the current financial position of the business and also an efficient decision-making process. Infrastructure as a Service model [30] of CA was mainly decided by resource metering and accounting. It entirely depends on CASP or third party for lease based.

Revised Manuscript Received on September 25, 2019

Dr.S.Gopalsamy, Assistant Professor, Department of International Business, Alagappa University, Karaikudi.

AV.Karthick, Teaching Assistant, Department of International Business, Alagappa University, Karaikudi

II. EXPLORING OF CLOUD ACCOUNTING

The major attractive feature of CA in advanced countries is due to the following reasons:

Zero maintenance

Existing hardware, software and network configuration are enough to run the day to day changing IT industry.

Bundle of accounting package

The client selects an accounting package from the large pool of Cloud Server. At any time, if the client wants any changes that are made possible.

Dashboard for cash inflow and cash outflow

Just single click the user views the entire information in the form of charts. Clients analyze the cash inflow and outflow in a user-friendly manner. This helps to predict and achieve the balance of payment.

Used in payroll processing, inventory management

Payroll processing and inventory management are processed using CA. Inventory management is an art. Both over-stocking and under-stocking lead to poor usage of resources.

III. MOTIVATION OF THE STUDY

Business point of view data is treated as an Asset. In the Recent days, the precious data are entered, stored, updated and submitted in Online for Taxation and Auditing purpose. This valuable data is hijacked by unidentified users. In Today’s IT field various modern trends have come into existence for solving real-time applications. Among them, CA is more familiar. It is applied in various fields like inventory, cash inflow, and cash outflow, marketing, sales, the financial position of the company and so on. Being gets more attracted by this technique the researcher like to correlate and extend this concept in Management Studies also. Based on this interest researcher, selected this research. Cloud Computing [9], [38], [39] is an efficient

DOI:10.35940/ijrte.B1071.0982S1019

cost-efficient strategy, in recent years that is adopted by many of the companies.

IV. EXISTING SYSTEM

Storage as a service (S3) is one of the recently added features of Cloud Computing. The rented S3 was classified on the basis of a number of months, storage space in GB, bandwidth, and operations. There is a huge possibility of data hacking and intruders attack the CA system. There is a zone of tolerance between the client and the CASP. The client expects a more secure, reliable and fault-free service at the lowest cost from the CASP. Service provider aims at low-cost operations and high availability of CA. 18% of the total companies in the worldwide using CA [22] report published by ACCA-IMA. CA has different types of issues like storage, bandwidth availability, security-based problems like reliability and privacy and heterogeneity of jobs. Today all information is stored in an electronic system. In business, they need a large volume of space for storing valuable data. They focus on how much privacy and reliability of accounting data.

The existing CA model was used to enter the data, billing, execute and store the data. Fingerprint-based systems are removed by human nerve based security mechanism that protects the data from unauthorized person. Cybercrime has faced new problems day by day. Hackers and intruders attacking the web page and create fake websites are seen in the online. There is a tug of war between the system developer/ professional and hackers/intruders. SLA [3] is used to maintain a smooth relationship between CASP and Clients.

Data security [17] as a crucial problem faced by the CA system, both CASP and client jointly work together to solve this security problem. CA is the migration of traditional accounting operations into Dematerialization [7] using an electronic platform. It is one of the emerging trend [36] using internets for accounting. It helps to differentiate the business from the competitive market. CA module [13] tries to achieve using the federated cloud for small datacenters management. CC has different types of issues [25] like storage, bandwidth availability, heterogeneity of jobs, security-related problems like reliability and privacy. Researchers take many efforts to solve these problems. Security is a set of technologies and policies to protect data and infrastructure.

V. PROPOSED SYSTEM FOR HIGHLY SECURED CLOUD ACCOUNTING

CA system is monitored and controlled by CASP based on SLA. Generally, the cloud offers various services like software, infrastructure, resources, platform, and storage. Among all the services, storage is the most challenging and debated service. Proposed work based on bio-metric based Iris, RSA and AES algorithm is used for an advanced security mechanism that protects the accounting data from intruders.

The figure 1 shows the Architecture of Efficient Double Secured Cloud Accounting for Business with an enhanced security model for CA protects precious accounting data. The client enter file into the CA platform, they ask user name and password at the time of logging into the system. CASP consists of a database server, a large number of VMs that has hardware layer and host layer. Usage tracking services used to identify data transactions.

The user is verified by biometric security. Then, the entered data file is converted into binary representation by using RSA and AES algorithms. While upload or download a large volume of file, the file is divided into number sub-segments, then encrypt the text in AES then it will be done by RSA algorithm.

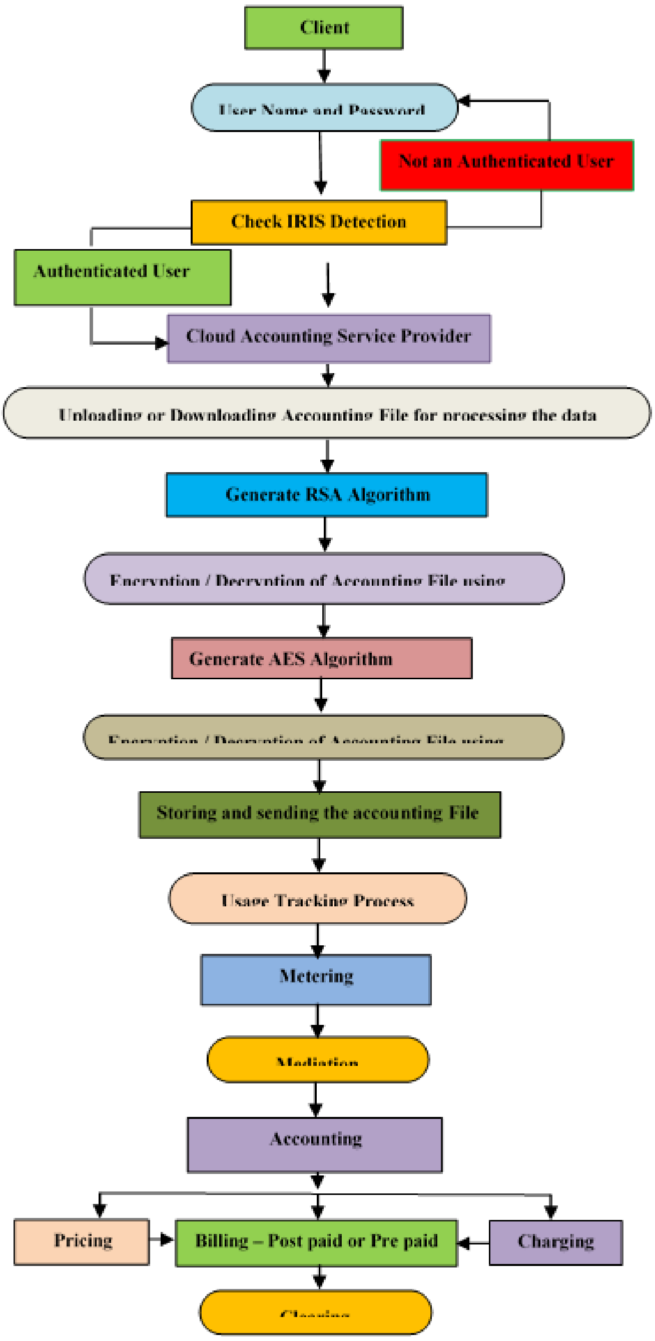
Client
User Name and Password
Not an Authenticated User
Check IRIS Detection
Authenticated User
Cloud Accounting Service Provider
Uploading or Downloading Accounting File for processing the data
Generate RSA Algorithm
Encryption / Decryption of Accounting File using
Generate AES Algorithm
Encryption / Decryption of Accounting File using
Storing and sending the accounting File
Usage Tracking Process
Metering
Mediation
Accounting
Pricing
Billing – Post paid or Pre paid
Charging
Clearing

Figure 1. The architecture of efficient high Secured Cloud Accounting

A. Iris Algorithm

A typical Iris recognition system designed [18] consists of four modules. Figure 2 shows the Architecture for Iris recognition system. The acquisition aims to capture high-quality Iris image.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Preprocessing consist of segmentation and normalization processes. In segmentation, it isolates the Iris region from the eye image. The normalization used to measure the varying size of the pupil. Feature encoding utilizes the texture analysis method to extract features from the normalized Iris image. The important features of the Iris are extracted as a series of binary codes known as digital biometric template. Finally, the matching module compares the user digital biometric template with all the stored templates in the database. The matching metric will give a range of values of the compared templates from the same Iris.

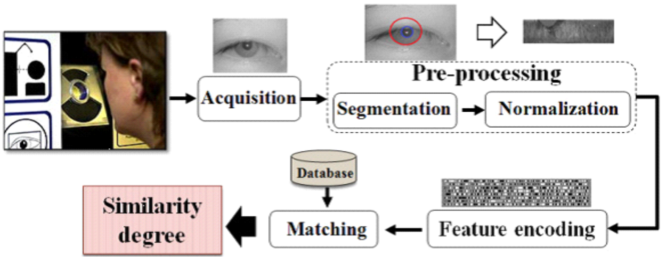

Figure 2. The architecture of iris recognition system

The Iris algorithm [16] is as follows:
1. Get an input image *I*.
2. Create a series of binned images so that

$I_k = B\{I_{k-1}, f\}, \qquad k = 1..K$

3. For *IK* (i.e. the most binned image in the series) find a minimum and assume it is a center ($x_0^{(K)}$, $y_0^{(K)}$) of the pupil. This step may require smoothing with a small (3x3) Gaussian mask. Set $r(K) = 2$; this is true for all CASIA images and in case the size of the most binned image is about 10 x 10 pixels. In other cases this value should be adjusted.
4. For each image $I^{(k)}$ k = 0..k starting from *K* to 0 (i.e. from more to less binned images)
(a) Construct a set of potential centers around the point defined by initial values obtained as the result of the previous stage

$$(x_0^{(k)}, y_0^{(k)}) \in C^{(k)}$$

Where

$C^{(k)} = \{(\hat{}x_{0\ \hat{y}}^{(k)} - [f_k/2])..(\hat{}x_0^{(k)} + [f_k/2])\} \times \{(\hat{y}_0^{(k)} - [f_k/2])..(\hat{y}_0^{(k)} + [f_k/2])\}$

(b) construct a set of potential radiuses

$$r^{(k)} \in \{(\check{r}^{(k)} - [f_k/2])..(\check{r}^{(k)} + [f_k/2])\}$$

(c) find (we omit the upper *k* index for editorial purpose)

$(\check{r}, \check{}x, \hat{y}) = \arg\max_{(r,x,y)} \sum_{m=1}^{M} (I_x(x_m, y_m) \cos\alpha_m + I_y(x_m, y_m) \sin\alpha_m)$

5. Recompute ($\check{r}^{(k)}, x^{\vee(k)}, \hat{y}^{(k)}$) to the finer grid using f_k

$$(\check{r}^{(k-1)}, x^{\wedge(k-1)}, \hat{y}^{(k-1)}) = f_k(\check{r}^{(k)}, x^{\vee(k)}, \hat{y}^{(k)})$$

In much the same way we search for external radius of an iris and for the center if required.

B. RSA Algorithm

RSA algorithm adopts the asymmetric method that has the public key [19] for encrypting the data. The private key is for decrypting the data. The client only knows the private key. In encryption, the plain text (original text) is converted into ciphertext. The cipher cannot read by normal users, whereas in decryption the ciphertext is converted into plain text. The key length is decided by the number of bits in the module. RSA algorithm [4] consists of three stages like Key generation, Encryption, and Decryption.

Key generation

Step1: Randomly choose two large prime numbers p and q

Step2: Compute $n = p \ast q$

Step3: Compute $z = (p - 1) \ast (q - 1)$

Using Euler's Totient function where z is the same as $\varphi(n)$

Step4: Choose e such that $1 < e < n$ and $e \equiv 1$ (modz)

Step5: Choose d such that $1 < d < z$ and $ed \equiv 1$ (modz)

Step6: P*ublic key is the pair (n,e) while Private key is the pair (n,d)

Encryption
Step7: $c = m^e \pmod{n}$, where $0 < m < n$, c is the ciphertext and m is the message

Decryption
Step8: $c^d \pmod{n}$

Step9: $m^e \pmod{n}^d \pmod{n}$

Step10: $m^{ed} \pmod{n} = m$ since $ed \equiv 1 \pmod{z}$ holds
Using Euler's Totient

$$\varphi(n, h) = \rho^h - \rho^0 \rho^h - \rho^1 \ldots \rho^h - \rho^h - 1 + q^h - q^0 q^h - q^1 \ldots q^h - q^{h-1}$$

C. AES Algorithm

With the help of password experiential [6], AES encrypt the data. The uniqueness of the RSA algorithm is a predefined key size like 128, 192 or 256 bits. The user uploads the accounting file from the cloud server for processing the information. RSA algorithm generates plain text into cipher text using encryption technique. In decryption, the ciphertext is converted into plain text. Afterward, the accounting data stored and send to the usage tracking system.

In these papers [12], [13] designed the hierarchy of CA. Metering is the topmost hierarchy in CA. Billing is also known as invoice. They process and collect charges for the transaction based on their resource utilized. Charging deals with cost calculation of resources utilized, storage, monthly used, bandwidth received, the technical units are converted into a currency value.

Key generation
Step1: Randomly choose two large prime numbers p and q

Step2: Compute $n = p * q$

Step3: Compute $z = (p - 1) * (q - 1)$ using Euler's Totient function
Step4: Compute
$\gamma(n, h) = \rho^h - \rho^0\rho^h - \rho^1 \ldots \rho^h - \rho^{h-1} + q^h - q^0 q^h - q^1 \ldots q^h - q^{h-1}$

Step5: Choose random integer r such that $1 < r < n$, $r \equiv 1 \pmod z$ and $r \equiv 1 \pmod{\gamma}$ where r is a small integer

Step6: Choose e such that $1 < e < z$ and $re \equiv 1 \pmod z$

Step7: Choose d such that $1 < d < \gamma(n)$ and $ed \equiv 1 \pmod{\gamma(n)}$

Step8: Public key is the pair (n,e)

Step9: Private key is the pair (n,d,r)

Step10: Choose a shared secret key s randomly

Encryption
Step11: if$(m < n)$ do

Step12: $c1 = ((m^{d1} \pmod n)^{d1} \pmod n)^s \pmod n$

Step13: $c2 = s^{e2} \pmod n$ where c is equal to the pair of (c1,c2)

Decryption
Step14: $s = c2^{d2} \pmod n$

Step15: After decrypting s, we can use s, r and e1 to decrypt c1 as shown: $(c1^r \pmod n)^{e1} \pmod n)^s \pmod n = m$.

VI. CONCLUSION AND FUTURE WORK

Provide maximum security is the foremost objective of the efficient security system. The proposed work helps to protect the most valuable Accounting data protected from intruders attack and brute force. It's a collaboration of biometric, Iris Algorithm, RSA and AES algorithms for protecting the data in a secured manner. The biometric-based Iris and encrypted security are cannot be hijacked by unauthorized users. Future work will focus on measure the size of the heart, as a biometric security for protecting the valuable data.

REFERENCES

1. Ahmed Mihoob, Carlos Molina Jimenez and Santosh Shrivastava, "A Case for Consumer Centric Resource Accounting Models", IEEE 3rd International Conference on Cloud Computing, pp. 506-512, 2010.
2. Ahmed Mihoob, Carlos Molina Jimenez, and Santosh Shrivastava, "Consumer Side Resource Accounting in the Cloud". IFIP, pp. 58-72, 2011.
3. Akhil Behl, Kanika Behl, "An analysis of Cloud Computing Security Issues", IEEE, pp. 109- 114, 2012.
4. Akshita Bhandari, Ashutosh Gupta, Debasis Das, "Secure Algorithm for Cloud Computing and Its Applications", IEEE, pp.188-192, 2016.
5. Anane Nadjia, Anane Mohamed, "AES IP for Hybrid Cryptosystem RSA-AES", 12th International Multi-Conference on Systems, Signals & Devices, IEEE, pp.1-6, 2015.
6. B.Venkatesh, V.Karthik, M.Gowtham, "Enhancing Network Security In Cloud Computing Using Cipher Cloud Mechanism", Proc. of ICICST, pp. 253- 256, 2016.
7. Bogdan, Iuliana, "Traditional Accounting Vs. Cloud Accounting", AMIS, pp. 106-125, 2013.
8. Ceslovas Christauskas, Regina Miseviciene, "Cloud Computing Based Accounting for Small to Medium Sized Business", Inzinerine Ekonomika-Engineering Economics, pp. 14-21, 2012.
9. AV.Karthick, Dr.M.Ayisha Millath, "Management of Digital Libraries for Active Learning Environment: Trends and Challenges", Library Philosophy and Practice, 2019.
10. Ewnetu Bayuh Lakew, Lei Xu, Francisco Hernandez-Rodriguez, Erik Elmroth, Claus Pahl, "A Synchronization Mechanism for Cloud Accounting Systems", IEEE International Conference on Cloud and Autonomic Computing, pp. 111-120, 2014.
11. Francis Pol C. Lim, "Impact of Information Technology on Accounting Systems", Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, pp. 93- 106, 2013.
12. Francisco Airton Pereira da Silva, Paulo Anselmo da Mota Silveira Neto, "Monext: An Accounting Framework for Infrastructure Clouds", IEEE 12th International Symposium on Parallel and Distributed Computing, pp. 26-33, 2013.
13. Francisco Airton Silva, Paulo Neto, Vinicius Garcia, Fernando Trinta and Rodrigo Assad, "Accounting Federated Clouds based on the JiTCloud Platform", 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, pp. 186-187, 2013.
14. Igor Ruiz Agundez, Yoseba K. Penya and Pablo G. Bringas, "A Flexible Accounting Model for Cloud Computing", Annual SRII Global Conference, pp. 277- 284, 2011.
15. Igor Ruiz Agundez, Yoseba K. Penya and Pablo G. Bringas, "Cloud Computing Services Accounting", International Journal of Advanced Computer Research, pp. 7-17, 2012.
16. Jan Mazur, "Fast Algorithm for Iris Detection", Springer-Verlag Berlin Heidelberg, pp. 858–867, 2007.
17. Jiao Feng, "Cloud Accounting: the transition of accounting information model in the big data background", In International Conference on Intelligent Transportation, Big Security and Smart City, pp. 207 – 211, 2015.
18. Juan M. Colores Vargas, Mireya Garcia Vazquez, Alejandro Ramirez Acosta, Hector Perez Meana and Mariko Nakano Miyatake, "Video Images Fusion to Improve Iris Recognition Accuracy in Unconstrained Environments", Springer-Verlag Berlin Heidelberg – MCPR, pp. 114-125, 2013.
19. K.Berlin, S.S.Dhenakaran, "A Novel Encryption Technique For Securing Text Files", Proc. of ICICST, pp. 179- 182, 2016.
20. Keke Gai, Longfei Qiu, Min Chen, Hui Zhao,Meikang Qiu, "SA-EAST: Security-Aware Efficient Data Transmission for ITS in Mobile Heterogeneous Cloud Computing", ACM Transactions on Embedded Computing Systems, pp.60-82, 2017.
21. Mihalache D, Arsenie Samoil, "Cloud Accounting", Ovidius University Annals, Economic Sciences Series, pp. 782-787, 2011.
22. Otilia Dimitriu, "Cloud Accounting – A New Player in the Economic Context", Economy and Management, pp. 727- 732, 2014.
23. Otilia Dimitriua, Marian Matei, "A New Paradigm for Accounting through Cloud Computing", Emerging Markets Queries in Finance and Business, pp. 840-846, 2014.
24. Otilia Dimitru, Marain Matel, "The expansion of accounting to the Cloud", SEA – Practical Application Science, pp. 237- 240, 2014.
25. Patil Madhubala R, "Survey on Security Concerns in Cloud Computing", IEEE, pp. 1458 – 1462, 2015.
26. P. Ravi Kumar, P. Herbert Raj, P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing", ICSCC - ScienceDirect - Procedia Computer Science, pp. 691–697, 2018.
27. Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahzad, "Multilevel classification of security concerns in cloud computing",Elsevier BV - Applied Computing and Informatics, pp. 57-65, 2016.
28. Talal Halabi, Martine Bellaiche, "A broker-based framework for standardization and management of cloud security-SLAs", Computers and Security, pp.1-41, 2018.

29. Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, Umberto Villano, “Security by design in Multi-Cloud Applications: An Optimization Approach”, Information Sciences, pp.1-47, 2018.
30. Varun Bhardwaj, Anamika Sharma, Gaurav Somani, “Client-Side Verifiable Accounting in Infrastructure Cloud”, IEEE, pp. 361- 366, 2015.
31. Wenjun Tang, “Key Technology analysis and application research of Accounting Informationization under Cloud Environment”, International Conference on Intelligent Transportation Big Data and Smart City, pp. 507 – 510, 2015.
32. Yaliang Zhao, Laurence T. Yang, Jiayu Sun, “A Secure High-Order CFS Algorithm on Clouds for Industrial Internet of Things”, IEEE Access, 2018.
33. Yan Yang, Xingyuan Chen, Hao Chen, Xuehui Du, “Improving Privacy and Security in Decentralizing Multi Authority Attribute Based Encryption in Cloud Computing”, IEEE Access, pp.1-17, 2018.
34. Zhang Cancan, “Challenges and Strategies of Promoting Cloud Accounting”, Eastern Academic Forum, pp. 90-94, 2014.
35. Zhengping Wu, Nailu Chu, Peng Su, “Improving Cloud Service Reliability - A System Accounting Approach”, IEEE Ninth International Conference on Services Computing, pp. 90 – 97, 2012.
36. Mozhdeh Sadighi, “Accounting System on Cloud: A Case Study”, 11th International Conference on Information Technology: New Generations, pp. 629- 632, 2014.
37. Minh T. Nguyen, Pavel. B. Khorev, “Information risks in the cloud environment and cloud-based secure information system model”, International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), IEEE xplore, 2019.
38. AV. Karthick, E. Ramaraj, R. Kannan, “An efficient Tri Queue job Scheduling using dynamic quantum time for cloud environment”, International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp. 871-876, 2013.
39. AV.Karthick, E. Ramaraj, R. Ganapathy Subramanian, “An Efficient Multi Queue Job Scheduling for Cloud Computing”, World Congress on Computing and Communication Technologies, pp. 164-166, 2014.
40. Erik Elmroth, Fermn Galan Marquezy, Daniel Henriksson, and David Perales Ferrera, “Accounting and Billing for Federated Cloud Infrastructures”, Eighth International Conference on Grid and Cooperative Computing, pp. 268 – 275, 2009.