



Cryptographic Techniques for Authentication of Cloud users for Secured Data Storage

¹C.G. Naveen Kumar and ²C. Chandrasekar

¹Bharathiar University,

Coimbatore,

India.

cgnaveenkumar11@gmail.com

²Govt. Arts College,

Udumalpet,

Tamilnadu, India.

chandrasekar2000@gmail.com

Abstract

Cloud computing is the idea actualized to break up the Daily Computing Problems. Cloud computing is essentially virtual pool of resources and it gives these resources to clients through web interface. Cloud computing is the web based improvement and utilized as a part of PC innovation. The common issue related with Cloud computing is information protection, security, obscurity and unwavering quality and so forth. Be that as it may, the most essential between them is security and how cloud provider guarantees it. Because of the tremendous measure of information storage on the cloud servers, cloud specialist organizations turn into an alluring target and may get numerous dangers. Security and protection are the key issues and difficulties for Cloud storage. In this paper, the proposed work design is to take out the uncertainties with respect to information protection, utilizing encryption calculations to upgrade the security in cloud according to alternate point of view of cloud clients. Encryption is an outstanding innovation for ensuring sensitive information. Cloud data centers are winding up progressively prominent for giving registering resources. In any case, the costs of these servers are expanded in processing limit with vast level of the operational costs because of vitality utilization, particularly in server center that are utilized as backend figuring framework for cloud computing. Utilization of the mix of Public and Private key encryption to conceal the sensitive information of clients, and content recovery. The Paper proposed a new technique for energy consumption reduction in cloud centers so that efficient computing

can be done. The paper also examines the plausibility of applying encryption calculation for information security and protection in cloud Storage. This paper primarily center around secured Cloud storage administrations i.e. Cryptography to give cryptographic methods to securing information and calculation in a cloud situation. Cryptography in Cloud computing is another safe administration with respect to security and protection in cloud. An improved validation component for distinguishing client in cloud condition is likewise proposed. There are three fundamental parts engaged with this structure in particular User, Trusted Authenticator (TA) and Cloud Service Providers (CSPs). The TA gives secure access to the client by creating the computerized mark and certifications. In this paper, the means for confirming the clients are additionally depicted.

Key Words: Privacy, encryption, decryption, cloud registering, security, Trusted Authenticator (TA), energy consumption, energy reduction.

1. Introduction

Cloud computing is an adaptable, practical and demonstrated conveyance stage for giving business or customer IT benefits over the Internet.

Cloud computing bolsters appropriated benefit arranged design, multi-clients and multi-area regulatory framework, it is more inclined to security dangers and vulnerabilities.

A noteworthy worry in cloud appropriation is its security and Privacy. Interruption prospects inside cloud condition are numerous and with high picks up. Security and Privacy issues are of more worry to cloud specialist organizations who are really facilitating the administrations. Much of the time, the provider must ensure that their foundation is secure and customers' information and applications are protected by executing security strategies and instruments.

The cloud can likewise be utilized to store archives either as a huge pool of reinforcement drive or as essential store of record storage. The servers utilized for Cloud storage are facilitated by third get-together organizations who work substantial server farms. When we buy in to Cloud storage we rent storage limit from the Cloud storage.

The information might be put away over different servers and at various areas. The "cloud" is made out of equipment, storage, systems, interfaces and administrations [1]. Clients can get to the registering power, framework, programming applications and administrations on request and they are free of areas. Cloud computing is a compensation for every utilization display that empowers constant conveyance of exceedingly versatile resources to various organizations utilizing the web.

Cloud computing gives customers a virtual registering framework which empowers them to store information and run applications. Cloud computing presents new security challenges as customer can't completely trust cloud providers. Cryptography in Cloud computing relies upon a protected Cloud computing engineering. Cloud computing is a processing model that is driven by economies of scale and is disseminated on huge scale. Cloud designs are created by most recent and dire requests. That is, the resources are progressively given to a client according to his demand ,and reclaimed after the activity is finished.

Security assumes an essential part in cloud, looked by the clients and additionally CSPs. The engineering of the Cloud computing includes various cloud parts collaborating with each other. In this way, it causes the client to get to the required administrations at a quicker rate.

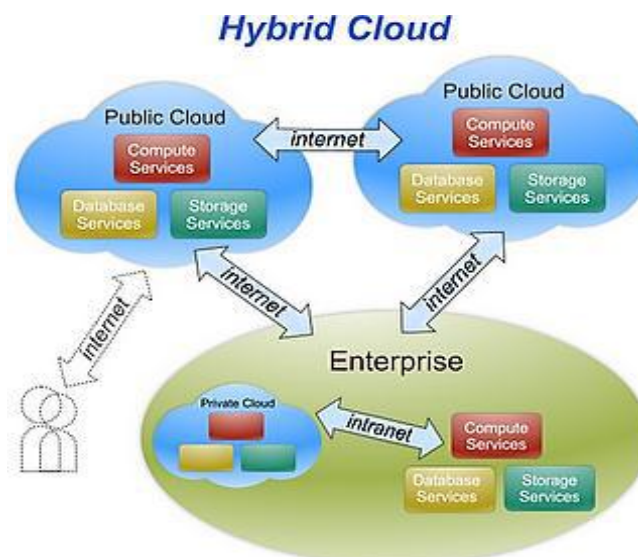


Fig. 1: Cloud Deployment Models

This paper proposes an upgraded verification instrument for validating the clients in cloud condition. In this structure, an idea of giving Digital Signature (DS) at the client level and furthermore in the Trusted Authenticator (TA) for high security is presented. Thusly, this model illuminates primary security issues like DOS Attack, DDoS Attack, Google hacking, listening stealthily, and so forth in a cloud domain. This model enables the client to get to the administrations from the cloud specialist organization side by confirming the entrance.

The target of this examination is to pick the best physical machine to reallocate cloud environment and to diminish of relocation of cloud memory keeping in mind the end goal to decrease energy utilization. To accomplish this objective, the Power Reduction Algorithm (PRA) will be adjusted to choose the fitting physical machine for reallocation and the calculation utilized as a part of [4] will be utilized to diminish the quantity of relocations.

1.1. Security Issues in Cloud Data Storage

- The physical security with the information is lost when we transfer the information in the cloud. The resources are additionally shared among various organizations. Clients don't have any learning or control of where the resources are running and where the information's are being put away.
- Though the information exchange, storage and recovery are done in light of approved exchange. Basic standard for information honesty not yet exist.
- The client's information individual information and data can be utilized or gone to different gatherings.

- The encryption and decoding is being finished by the cloud specialist co-op and even the keys are with them. Clients don't have any control on their information once the information are being submitted to the cloud specialist organization. Legitimately the keys ought to be available with the clients.

The above security issues talked about above demonstrates that there are different strategies issues and dangers exhibit in Cloud computing innovation. These issues incorporate protection, information isolation, unwavering quality, storage, security, get to control and some more. Investigating the distinctive issues we understood that security is one of the principle issues. It might be any venture information, a scholastics information or any basic clients information, security is the fundamental issue is security. So we can propose some encryption calculation utilizing some learning of existing calculation.

2. Literature Survey

These days, a few number of investigates on security issues in Cloud computing are being done. Different security systems are proposed by various analysts. By breaking down those works, some security issues are distinguished and few works are considered for proposing another system to verify the client for getting to secure administrations from the cloud specialist co-op.

Yashpalsinh Jadeja et al.[1] proposed Agent Based approach for Authentication in the Cloud (ABAC) to validate the clients for getting to the cloud administrations and furthermore to lessen the inward and outside assaults. In cloud condition, the VMware parts included are VMware ESX, VCenter Server, and Active Directory Server. The stages engaged with the ABAC design are Registration Phase, Key Generation and Distribution Phase and Authentication and Verification stage. The benefit of the ABAC is; it given an additional layer of security for the whole cloud. The significant disservice is; it doesn't give versatile validation foundation.

Naveen Dogra et al.[2] proposed a confide in demonstrate for cloud engineering. It utilizes the portable operator which is utilized as a security specialist and it screens the respectability and genuineness. This framework remotely screens and authenticates the trustworthiness of vital framework records, therefore filling a hole in the Xen Cloud Platform. This was its significant favorable position. Additionally specialist co-op can guarantee satisfaction of security strategies by staying away from assaults on VMs. The disadvantage of the proposed show is; it gives secure and dependable correspondence just through a portable specialist not through operators introduce in the cloud condition.

V.Nirmala et al.[3] proposed a model for trusted registering and illuminate the data fraud in the cloud and it was mimicked in the .Net condition. The assessment of the proposed display happens in three ways: security breaking

down, reproducing, and BLP private. The model includes six stages on the Open ID trade of information stream. The quality of the proposed show is assessed against phishing assaults and it brings about an ideal arrangement. The constraint of the proposed demonstrate is it was assessed just in united condition and it was its downside.

Pradnyesh Bhisikar et al. [4] proposed a power-mindful system for a heterogeneous virtual condition. They utilized equipment systems, for example, dynamic voltage and recurrence scaling and virtualization to oversee vitality. A worldwide chief is characterized to assign new Virtual Machine(VM) and reallocate relocated VM. The relocation cost is ascertained utilizing the extent of VMs. The creators likewise analyzed a few calculations for tackling the power enhancement issue.

Sarika Gupta et al.[5] proposed a model consolidating powerful cud click focuses, alphanumerical validation, sound mark and attract a-mystery request to conquer the ease of use and security. This framework is the blend of graphical watchword, content, draw-a-mystery strategy and telephone message, which increment the certainty and unwavering quality. This was the upside of the proposed framework. The detriment was that there is precariousness happens in information storage for cloud.

P. Fanfara et.al [6] coordinated the hubs utilizing the VM movement calculation in green cloud figuring. Since movement costs a great deal for the cloud provider, the second objective of the creators was to limit the quantity of relocations. Their approach outflanks the container pressing heuristic calculations, for example, the principal fit diminishing calculation.

3. Crypto Cloud Computing

Crypto Cloud computing is another system for digital asset sharing. It ensures information security and protection. All things considered, in cloud condition, crypto Cloud computing ensures the data security and trustworthiness amid entire strategy. Security administration of Cloud computing can likewise be performed by approving the marks of each component included. What's more, a client can recover every single related asset utilizing his QDK key. There is no individual security under the present cloud structure, as pointed out by Mark Zuckerberg, 'the Age of Privacy Is Over'. [7]However, with the advancement of crypto Cloud computing, we can resolve the contention between administrations information sharing and protection security. It opens up new prospects for the improvement of data sharing innovation.

4. Proposed Framework

The proposed system for validating the client in cloud stage. In this model, an idea of giving a Digital Signature (DS) at the client story and a Trusted Authenticator (TA) for giving high security is displayed. This model enables the

cloud client to get to the administrations from the cloud specialist organization's by verifying the entrance demands. The correspondence between the client and the CSPs are validated by the Trusted Authenticator (TA). The trusted authenticator confirms the client and enables the client and CSP to convey in getting to the administrations.

The TA has two stages, one was the Registration stage and another was the confirmation stage. The TA has a database server which checks for enlisted client and approves the client to get to administrations from CSP. On the off chance that the client isn't an enrolled customer, it makes an impression on the invalid customer. The TA likewise gives an advanced mark, which gives higher security level of getting to administrations.

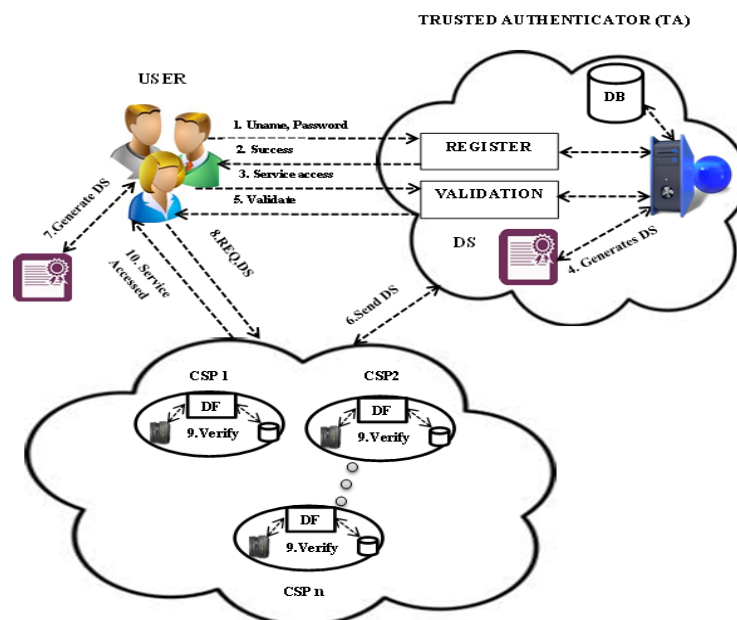


Fig. 2: Proposed Authentication Mechanism

At the point when the client gets approved, he is allowed to approach the CSP for requesting the administrations alongside the Digital Signature. The program on the client side has an extra which creates the Digital Signature of similar qualifications in which the TA produces, and the Digital Signature wraps the client ask. The client demands for getting to administrations alongside Digital Signature will be sent to the CSP.

The billows of CSP have the demand from the client side and the DS from the TA and apportion the regarded CSP which has the asked for administrations. The regarded CSP has an operator who checks the DS from both client and CSP. In the event that they are equivalent, at that point the client is permitted to get to the administration effectively.

4.1. Proposed Algorithm

The proposed algorithm provides high security to the data in cloud by performing cryptographic mechanisms. The proposed algorithm provides security to the data.

```

Step 1: Input CU1 & TA
Step 2: Divide CU1 = L & R
Step 3: Divide TA = 1K64 & 2K64
Step 4:  $CU \gg r \rightarrow CU$  (2-bit Right Circular shift)
Step 5:  $CU \oplus CP \rightarrow CU$  (XOR operation)
Step 6:  $CU \gg r \rightarrow CU$  (2-bit Right Circular shift)
Step 7: Swap CU & CP
Step 8:  $CU \oplus 1K64 \rightarrow CU$ 
Step 9:  $CU \ll 1 \rightarrow CU$  (2-bit Left Circular shift)
Step 10:  $CU \oplus CP \rightarrow CU$ 
Step 11:  $CU \ll 1 \rightarrow CU$  (2-bit Right Circular shift)
Step 12: Swap CU & CP
Step 13:  $CP \oplus 2K64 \rightarrow CP$ 
Step 14: Repeat step 4 to 13 up to n rounds where n is no. of cloud users
Step 15:  $CU + CP = CD$ 

```

The algorithm for validating cloud users is given below.

```

Step 1: Start
Step 2: Enter key K and id  $\alpha$ . (for the authentication of the user) by Trusted Authority(TA).
Step 3 : User key K and id  $\alpha$  reach at Trusted Authority End.
Step 4: Check Authentication
    Step 4.1: By matching K and  $\alpha$  at the cloud storage.
    Step 4.2: If user gets authenticated at step 4.1, then cloud security system goes next step.
            Otherwise Cloud Security system disallows the user to get accessing rights to
            the file.
Step 5: Prepare AL by applying algorithm.
Step 6: Generate initial level cipher text,  $CT_1$  such that,  $CT_1 = CT_1$  .
Step 7: Generate user Text data, T such that  $T' = T$ .
Step 8: Send User text back to user at the user end (at another end of cloud environment).
Step 9: Stop

```

The working of the algorithm is explained below

Stage 1. The client sends his username and secret word for enlistment to the Trusted Authenticator.

Stage 2. Put stock in Authenticator (TA) enlists the client accreditations and answer achievement of enrollment.

Stage 3. Once more, after enrollment the client sends the demand of a support of the Trusted Authenticator.

Stage 4. TA approves the client and makes a computerized signature for the demand made alongside client qualifications.

Stage 5. TA communicates something specific of progress, or access denied, as indicated by the foundation.

Stage 6. TA sends the computerized mark to the CSP's cloud.

Stage 7. Client gets approved and make the computerized signature from the client side for the demand he made alongside his certifications.

Stage 8. The client sends his demand alongside the advanced mark to the CSP's cloud.

Stage 9. Each CSP has an operator who breaks the computerized mark of client and confided in authenticator, and if both acknowledge the same advanced mark, CSP gives the section of the client ask.

Stage 10. Client profits the administration as indicated by the demand.

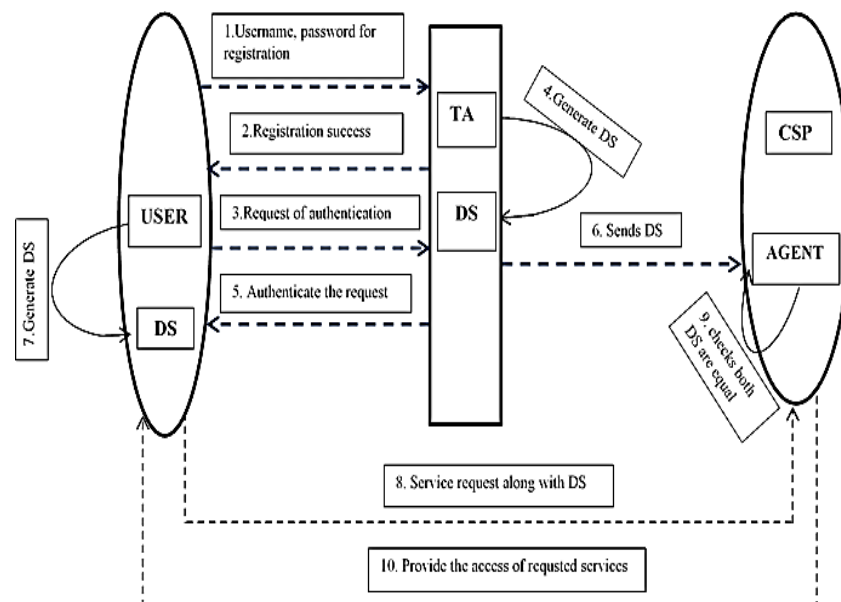


Fig. 3: Workflow of Authentication Mechanism

4.2. Proposed Method for Power Reduction

This paper goes for vitality effectiveness in the foundation as an administration (IaaS) level. The principle strategy utilized for enhancing the effectiveness of assets in the server farms is virtualization. The proposed approach decreases the cloud memory movement and vitality utilization, utilizing dynamic arrangement of relocated VMs. This approach has four stages:

1-Sorting the hosts in diving request by their work loads

2-cloud memory are chosen from the low load have for movement and are

arranged in diving request by their positioning in the rundown of movement. It is important that there is a plausibility of movement if all memory slots can move from the thought about host. On the off chance that this is unimaginable for a solitary memory location, there is no relocation from that host.

3-Placing the cloud data from the rundown of relocation to the objective host considering the limit of 70% .

4-Shutting down the low load memory slots and reassign energy units.

This examination centers around cloud memory placement. cloud memory arrangement can be considered as the container pressing issue, in that the containers are the hosts and parcels are memory slots. Since container pressing is a NP-hard issue [34], heuristic techniques are utilized to settle them.

5. Results

The proposed algorithm which performs cryptographic mechanisms performs better when compared to traditional methods and the results show that the proposed better and provides high level of security.

The performance levels of security is illustrated as below.

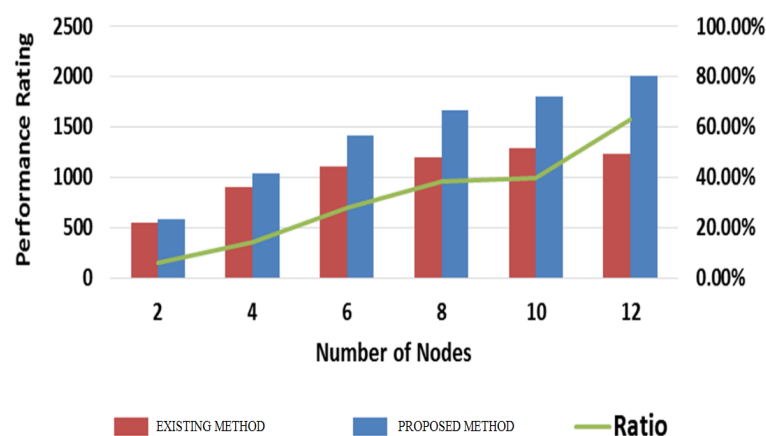


Fig. 4: Performance Comparison

The energy comparison of cloud users based on no.of joules is calculated and depicted in below figure

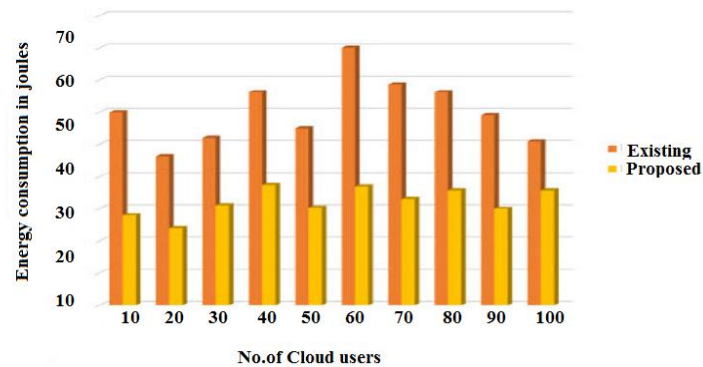


Fig. 5: Energy Consumption Levels

The energy level consumption is reduced when power reduction algorithm is applied on cloud data providers and service providers. The rate of power reduction is illustrated in table below.

Table 1: Processor Load

CPU Load	Proposed Method	Existing Method
0%	86	93.7
10%	89.4	97
20%	92.6	101
30%	96	105
40%	99.5	110
50%	102	116
60%	106	121
70%	108	125
80%	112	129
90%	114	133
100%	117	135

6. Conclusions

The Cloud processing as an innovation would be embraced if the zones of concerns like security of the information will be secured with full evidence component. The quality of Cloud computing is the capacity to oversee hazards specifically to security issues. The proposed system represents the means for getting to the administrations. Along these lines, the client is in charge of verify himself with the TA and allowed to get to the administrations as per his demand. Computerized Signatures brings the largest amount of security. With a specific end goal to keep the interloper demonstration amid the travel Digital Signature from TA to client, the idea of making the DS on the client side is connected. Accordingly, the DS is recently made at the client agree with a similar qualification made by TA. The proposed power reduction algorithm is

applied on cloud users for power reduction so that cloud users can effectively make use of cloud services. Our recommended model will introduce a diagram portray of engineering to be received by planners engaged with actualizing the Cloud computing. Security calculations said for encryption and unscrambling and routes proposed to get to the media substance can be executed in future to improve security system over the system. Later on, we will endeavor to investigate our exploration by giving calculation usage and creating results to legitimize our ideas of security for Cloud computing. All together for this way to deal with fill in as expected, the cloud specialist organization must co-work with the client in executing arrangement. Some cloud specialist co-ops construct their plans of action with respect to the offer of client information to sponsors. These providers presumably would not enable the client to utilize their applications in a way that jelly client security.

References

- [1] Yashpalsinh Jadeja and Kirit Modi," Cloud Co mputing - Concepts, Architecture and Challenges" IEEE [2012].
- [2] Naveen Dogra and Harpreet Kaur," Cloud Computing Security: Issues and Concerns," .
- [3] V.Nirmala, R.K.Sivanandhan and DR.R.Shanmuga lakshmi, "Data Confidentiality and Integrity Ve rification using User Authenticator Scheme in cloud , proceeding of 2013 International Conference on Green High Performance Computing , IEEE, 2013.
- [4] Pradnyesh Bhisikar , Prof A mit Sahu ,"Security In Data Storage and Transmission In Cloud Compituing,International Journal Of Advanced Research In Cloud Science And Software Engineering, IJARCSSE, March 2013.
- [5] Sarika Gupta, Sangita Rani Satapathy ,Piyush Mehta and Anupam Tripathy," A Secure and Searchable Data Storage in Cloud Co mputing" IEEE [2012].
- [6] P. Fanfara , E. Dankova and M. Dufala ,"Usage of Asymmetric Encryption Algorithms to Enhance the Security of Sensitive Data in Secure Co mmunicat ion" IEEE [2011].
- [7] Chandramohan.D, Vengattaraman.T, Rajaguru. D, Baskaran.R and Dhavachelvan"A Privacy Breach Preventing And Mitigation Methodology For Cloud Serv ice Data Storage", IEEE [2012].
- [8] Rene Leistiko w & Djamshid Tavangarian, "Secure Picture Data Part itioning for Cloud Co mputing Services"IEEE [2013].
- [9] Deepak Harjani, Mohita Jethwani , Nitika Keswaney and Sheba Jacob, "Automated Parking Management system Using License Plate Recognition, IJCTA, sep-oct 2013.

- [10] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu, "Secure Storage and Access of Data in Cloud Computing", IEEE2012, P. 336-339.
- [11] Bao Zhang, Changgen Peng, Zhipin Xu "Identity-based Cloud cloud storage encryption scheme", IEEE 2011, pages 610-614.
- [12] Mengmeng Wang, Guiliang Zhu, Xiaoqiang Zhang, "General Survey on Massive Data Encryption", P. 150-155.
- [13] M.Sudha, M.Monica, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012, P. 32-37.
- [14] Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, 2012, p. 179-183
- [15] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms" Vol. 8, 2009, p. 58-64.
- [16] S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9, 2003.
- [17] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, P. 84-89.
- [18] Nicholas Jansma, Brandon Arrendond, "Performance Comparison of Elliptic Curve and RSA Digital Signatures" April, 2004.
- [19] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography" vol. 2 Issue 3, July 2012.

