International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Enhanced Integrity Preserving Homomorphic Scheme For Cloud Storage

Payal Gupta[1] , Mr. Vivek Sharma[2]

[1]*Research Scholar, Department Of Computer Science and Engineering , JMIT, Radaur, Haryana, India*
[2]*Assist. Professor, Department Of Computer Science and Engineering , JMIT, Radaur, Haryana , India*

Abstract- *Confidentiality and integrity are the majority vital subjects in cloud storage space scheme. After user uploads his data and deletes innate duplicate, he could capitulated utmost manipulation of data. This paper audits different difficulties and takes a shot at cloud honesty safeguarding plans. The proposed plan can ensure privacy of messages for a drawn out stretch of time. Also we extend the calculation to bolster multiparty calculation while protecting its homomorphic properties. In this work, we are going to analysis fully Homomorphic schemes for encryption and integrity check using MD5 Algorithm.*

Key Words: **Cloud Computing, Security and Integrity, Storage and Security, Privacy, Vulnerabilities etc.**

1. Introduction

The Cloud computing, as an growing computing example aiming to allocate storage, totaling, and services transparently amid an large users, have gathered outstanding impetus from not merely manufacturing but additionally academe. In core, the cloud computing [1] overlap countless continuing thoughts, such as dispersed, grid and value computing. Though, ambitious mainly via promotion and ability donations from large company contestants like Google, IBM Amazon, the cloud computing has evolved out of these thoughts with come to be a new noise speech concentrating on "cloud"—extra hypothetical supply and services' delivery. After cloud computing stepladder into our every day lifetimes, each innately store data, such as email, word meting out documents and spreadsheet might be distantly stored in a cloud. Then, we preserve use both terminals, e.g., computer, laptop and PDA etc., to admission this data at anytime, where. The "cloud" in cloud computing can be described as put of hardware, webs, storage, services, and interfaces to join to hold aspects of computing as a repair[2][3]. The Cloud services contain transport of multimedia, groundwork, and storage space above Internet established on consumer require. The Cloud computing has four vital personality: elasticity and skill to scale up and downward, self-service provisioning and regular DE provisioning, request software design interface (APIs), bill and metering of ability custom inside a pay-as-you-go ideal. The Cloud computing can completely modify technique firms employ knowledge toward ability clients, associates, and supplier. A little company, such as Google and Amazon, by now has mainly of their IT resources in the cloud. They have discovered that it can remove countless of the convoluted constraint from the established compute nature, encompassing liberty, period, domination, and price [4].

1.2 Privacy in Cloud Computing

When a consumer stores a little receptive data in a cloud, privacy of this receptive data is of worry to user. Lacking each guard on this susceptible data, e.g., confidential commercial data, condition -records, a user won't boast assurance in store his/her aware data in make unclear. likewise, after an firm provisions a little company papers, e.g., company strategies, inside a cloud, firm additionally care concerning the privacy hopes merely pertinent workers be able to admission these papers afterward they are official. As well confidentiality of these responsive data, user's individuality solitude, a frank correct to isolation, is as well anticipated in cloud compute. If admission to a cloud discloses a user's genuine individuality, the consumer might yet live reluctant near accord this paradigm. Due to these grounds, the user validation lacking recognizing the actual individuality, additionally shouted nameless authentication, is attractive in cloud computing. Even though nameless verification know how to furnish consumer individuality privacy, it is a two-edged blade to furnish finished nameless admission in cloud computing. For instance, after a cluster of users are official to a little profitable computing and data-intensive sound collaborations in a cloud, if an vital data attuned by a celebrity is challenge, it is hard to track the real consumer unpaid to inclusive nameless authentication. Thus, to tackle this predicament, cloud compute ought to moreover furnish provenance to proof ownership and process past of data substance in cloud in arrange for open agreement to public. Safe provenance is vital to accomplishment of data forensics in cloud computing, yet it is a challenging theme today. Aiming at this, we counsel a safeguard provenance method established on bilinear pairing technique to supply trusted evidences for data forensics in cloud compute. Concretely, this paper will create pursuing contributions:

- initially, the formal definition and security notions of locked origin for cloud computing are introduced;
- Secondly, based on Diffie Hellman bilinear pairings scheme, an abstract provenance strategy is proposed,

which can gain information confidentiality, anonymous access to cloud, and conditional origin tracking;
- Thirdly, we use demonstrable security method to validate its security in standard model.

2. Data Integrity over Cloud

Integrity, in words of data defense, is nothing but promise that data can just be accessed and adjusted by those authorized to do so, in simple word it is procedure of verifying data. Data Integrity is extremely vital among supplementary cloud challenges. As data integrity gives promise that data is of elevated excellence, right, unmodified. Later storing data to cloud, user depends on cloud to furnish further reliable services to them and hopes that their data requests are in safeguarded manner. But that yearn could flounder from time to time user's data could be modified and deleted. Sometimes, cloud ability providers could be dishonest and they could discard data that has not been accessed and scarcely accessed to save storage space and retain less replicas than promised. Moreover, cloud ability providers could select to hide data defeat claim that data are yet accurately stored in the Cloud. As a consequence, data proprietors command to be convinced that their data are exactly stored in Cloud. So, one of the major concerns alongside cloud data storage is that of data integrity verification at untrusted servers.

3. Literature Survey

Zhifeng Xiao et al, in "protection and privacy in Cloud Computing" 2013 [5], the authors describe recent advances have given upward thrust to the status and success of cloud computing. However, when outsourcing the information and business utility to a 3rd social gathering motives the safety and privateness problems to grow to be a relevant main issue. For the duration of the learn at hand, the authors obtain a usual purpose to provide a complete evaluation of the present safety and privacy problems in cloud environments. They have got identified five most representative protection and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privateness-preservability). Establishing with these attributes, they gift the relationships amongst them, the vulnerabilities that could be exploited through attackers, the chance models, as good as existing security procedures in a cloud situation. Future study directions are earlier decided for every attribute.

Pitropakis, N. Et al, in "it can be All within the Cloud: Reviewing Cloud safety" 2013 [6], the authors describe Cloud computing is step by step replacing usual IT infrastructures. Nevertheless, an principal difficulty that has emerged by means of that revolution is the maintenance of an sufficient level of security for the infrastructure. Presently there are lots of researchers working within the discipline of cloud safety and privateness safeguard, proposing a few solutions that tackle the threats towards cloud infrastructures. This paper presents a radical overview of the study work within the field imparting the solutions that have been proposed thus far.

Alabool, H.M. Et al, in "usual believe standards For IaaS cloud analysis and resolution" 2014 [7], the authors describe As Infrastructure as a provider (IaaS) cloud becomes increasingly predominant to all stakeholders; the evaluation on the measure of trust of the IaaS cloud remains a undertaking. This gain knowledge of ambitions to observe and determine the common believe standards (CTC) from context-headquartered believe and context-situated cloud and later geared up, discussed, when put next, and aggregated a conceptual mannequin of CTC in an neutral manner. The most important purposes of CTC mannequin are: (a) to provide Cloud carrier Requesters (CSRs) with a CTC mannequin with which to evaluate the degree of believe that can be positioned in IaaS cloud (b) to furnish steerage to Cloud carrier providers (CSPs) as to what to construct into their new, widely-available depended on IaaS cloud to be able to satisfy trust specifications. To take action, a scientific evaluate on context established believe and context-headquartered cloud is provided. The results indicated that there was an principal set of believe standards comparable to Integrity, Benevolence, and fame that were uncared for from the present research related to cloud.

Hazarika, P. Et al, in "The mobile-cloud computing (MCC) roadblocks" 2014 [8], the authors describe Cloud computing is a quality trade thought and prior to now a long time this suggestion has blossomed right into a major segment in IT enterprise. Corporations, without reference to dimension, have both adopted cloud or planning to undertake cloud. In trendy Smartphone technology, cellular science is a best suit to leverage cloud computing, the later inherently addressing the boundaries of the former. With cloud computing, knowledge and related processing can also be offloaded to cloud and the processed know-how can also be consumed via mobile devices. This collaboration is aptly named as mobile cloud computing. To make the mobile cloud ecosystem to work seamlessly is a significant undertaking in itself. Adopting cloud implies placing business vital purposes and touchy data out to a 3rd party cloud dealer, which has essential security implications. With cell gadgets, the risk is also more suitable than ever. This paper discusses the quite a lot of cellular cloud challenges that pose competencies roadblocks for cellular cloud collaboration.

Selvakumar, C. Et al, in "PDDS - making improvements to cloud information storage protection using knowledge partitioning method" 2013 [9], the authors describe Cloud storage process permits storing of knowledge within the cloud server successfully and makes the user to work with the info with none situation of the assets. Within the present approach, the info are stored in the cloud using dynamic knowledge operation with computation which makes the

consumer have got to make a copy for further updating and verification of the data loss. An effective disbursed storage auditing mechanism is deliberate which over comes the boundaries in dealing with the information loss. In this paper the partitioning approach is proposed for the info storage which avoids the regional replica at the user side by way of making use of partitioning method. This process ensures excessive cloud storage integrity, greater error localization and handy identification of misbehaving server. To attain this, faraway information integrity checking suggestion is used to increase the performance of cloud storage. In nature the information are dynamic in cloud; as a result this work aims to retailer the info in decreased space with less time and computational cost.

4. PROPOSED WORK

4.1 Problem Identification

Cloud Computing brings unprecedented image shifting and benefits in the history of IT. As Cloud Computing becomes prevalent, much more sensitive information are being centralized into the cloud, such as emails, personal health records, private videos and photos, company finance data, government documents, etc. Users by storing the data into the cloud data storage, can be relieved from the burden of storing data and maintenance so as to enjoy the on-demand high quality data storage service. However, the fact that owners of data as well as cloud server are not in the same trusted domain may put the outsourced data at risk, as the cloud server may now not be fully trusted in such a cloud environment due to a number of reasons: the cloud server may leak data information to unauthorized entities or be hacked. It follows that for data privacy and combating unsolicited accesses sensitive data should be encrypted prior to outsourcing. In cloud computing cloud users and cloud service providers are almost certain to be from different trust domains. Data security and privacy are the critical issues for remote data storage.

4.2 Proposed Work

A simple resolution is employing user hidden key to encrypt file, but it is risky that user grasp merely key. After the key is capitulated and compromised, user cannot elucidate the data. At alike period, relying on one key could cause association difficulty. Because key is extra facilely stolen after it is just retained by user, so it will raise chance of data leakage. Threshold Bilinear Diffie Hellman (proposed in basepaper) is known to be capable to person-in-the-middle aggressions and this can be circumvented (as for instance completed in TLS) by authenticating Diffie Hellman whichever

- adding the parameters of Diffie Hellman which have static values say (p,g,gb) of one party (the server in TLS) into a certificate which is signed by a trusted authority (where the static parameters stay same for all key connections) and
- by requiring the server to sign ephemeral Diffie-Hellman key, i.e., gb where b is selected randomly for every new interaction, sent to extra party (the client). Thereby, public verification key corresponding to signing key is put into a certificate which is signed by a trusted authority.

We counsel a safeguard data integrity checking decentralized erasure series cloud storage agreement established on Elative allocate scheme. Our storage arrangement that consists of storage servers and key servers can completely stop malicious servers from robbing our data that are partly decrypted. The counseled system can promise confidentiality of memos for a long age of time.

We will use a homomorphic encryption system that permits increasing plaintext hidden inside of cipher texts and after employing homomorphism property alongside an encryption of individuality agent 1 of cluster permits to openly re-randomize cipher texts, i.e., attain new cipher texts for the alike memo that are unlikable to early on cipher texts. Employing exponential Key obtained from Key Transactions by encoding message.

Main supremacy in counseled work is that in arrange to decrypt an encrypted memo; countless parties (extra than a little threshold number) have to cooperate in decryption protocol.

4.3 Diffie–Hellman key agreement

For example, Alice, Bob, and Carol might give in a Diffie–Hellman accord as follows, alongside every procedure seized to be modulo p:

1. Firstly parties agree on algorithm parameters p and g.
2. The parties generate their private keys, named a, b, and c.
3. Alice computes g^a and sends it to Bob.
4. Bob computes $(g^a)^b = g^{ab}$ and sends it to Carol.
5. Carol computes $(g^{ab})^c$ ie. g^{abc} and uses outcome as her secret.
6. Bob computes g^b and then sends it to Carol.
7. Carol computes $(g^b)^c = g^{bc}$ and sends result to Alice.
8. Alice computes $(g^{bc})^a = g^{bca} = g^{abc}$ and uses it as her secret.
9. Carol computes g^c and sends it to Alice.
10. Alice computes $(g^c)^a = g^{ca}$ and sends it to Bob.
11. Bob computes $(g^{ca})^b = g^{cab} = g^{abc}$ which he uses as his secret.

An eavesdropper cannot use any combination to efficiently reproduce g^{abc}.

4.4 Threshold Based Data integrity Checking for Cloud Storage

Users store their vital data in cloud, such as pictures and documents. A cloud storage arrangement is believed as a major distributed storage arrangement composed of countless autonomous storage servers, such as Amazon easy storage service. The development is as follows: a message M is divided into k equal span blocks, then forms a vector M= (M_1, M_2, . . . M_k). We use erasure encode to create M redundant to get code word of a vector C= (C_1, C_2, . . ., C_n) by via erasure code (n, k). N of C_i are stored in n storage servers. To retrieve message M, we choose randomly k of C_i from n storage servers by using erasure code (n, k). Note that all of m_i must be collected, then encoded to form C_i. So erasure code (n, k) is a center of this storage system.

4.5 Homomorphic Scheme for Cloud Integrity

Homomorphic Encryption arrangements are utilized to current procedures on encrypted data lacking knowing confidential key (without decryption); client is merely holder of the hidden key. After we decrypt consequence of each procedure, it is the alike as if we had grasped out the calculation on the raw data. Homomorphism encryption (only additions of the raw data) is cryptosystems, and multiplicative Homomorphism encryption (only products on raw data) is basically RSA and El Gamal cryptosystems.

- E k is an encryption algorithm with key k.
- Dk is a decryption algorithm.

$$D_k(E_k(n) \times (E_k(m)) = n \times m \; OR \; Enc\,(x \otimes y) = Enc(x) \otimes Enc(y)$$
$$D_L(E_L(n) \times (E_L(m)) = n \times m \; OR \; Enc\,(x \otimes y) = Enc(x) \otimes Enc(y)$$

Multiplicative Homomorphic Encryption (RSA cryptosystem):

Let $n = pq$ where p and q are primes. Pick a and b such that $ab \equiv 1 \pmod{\phi(n)}$. n and b are public while p, q and a are private.

$$e_k(x) = x^b \bmod n$$

$$d_k(y) = y^a \bmod n$$

The Homomorphism: Suppose x 1 and x 2 are plaintexts.

Then,

$$e_k(X_1)e_k(X_2) = X_1^b X_2^b \bmod n = (X_1 X_2)^b \bmod n = e_k(X_1 X_2)$$

Additive Holomorphic Encryption:

Pick two large primes p and q and let $n = pq$. Let λ denote the Carmichael function, that is, $\lambda(n) = \text{lcm}(p-1, q-1)$. Pick random $g \in Z^*_{n^2}$ such that $L(g^\lambda \bmod n^2)$ is invertible modulo n (where $L(u) = \frac{u-1}{n}$). n and g are public; p and q (or λ) are private. For plaintext x and resulting ciphertext y, select a random $r \in Z^*_n$. Then,

$$e_k(x, r) = g^x r^n \bmod n^2$$

$$d_k(y) = \frac{L(y^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$$

The Homomorphism: Suppose x1 and x2 are plaintexts. Then,

$$\begin{aligned} e_k(x_1, r_1)\, e_k(x_2, r_2) &= g^{x1}\, r_1^n \cdot g^{x2}\, r_2^n \bmod n^2 \\ &= g^{x1+x2}\, (r_1\, r_2)^n \bmod n^2 \\ &= e_k(x_{1+}\, x_2,\, r_1 r_2) \end{aligned}$$

We present multiplicative homomorphism cryptosystem that is basically El Gamal cryptosystem but by modifying coding mode we can create it additive.

El Gamal Cryptosystem:

Let p be a prime and pick $\alpha \in Z^*_p$ such that α is a generator of Z^*_p. Pick a and β such that $\beta \equiv \alpha^a \pmod p$. p, α and β are public; a is private. Let $r \in Z_{p-1}$ be a secret random number. Then,

$$e_k(x, r) = (\alpha^r \bmod p, x\beta^r \bmod p)$$

El Gamal Cryptosystem performs multiplicative homomorphic encryption propriety: Let x 1 and x 2 be plaintexts. Then,

$$\begin{aligned} e_k(x_1, r_1)\, e_k(x_2, r_2) &= (\alpha^{r1} \bmod p,\, x_1 \beta^{r1} \bmod p)(\alpha^{r2} \bmod p,\, x_2 \beta^{r2} \bmod p) \\ &= (\alpha^{r1+r2} \bmod p,\, (x_1\, x_2)\, \beta^{r1+r2} \bmod p \\ &= e_k(x_1 x_2,\, r_1 r_2) \end{aligned}$$

If we put the plaintext in the exponent, we get:

$$e_k(x, r) = (\alpha^r \bmod p,\, \alpha^x\, \beta^r \bmod p)$$

Then the homomorphism is additive:

$$\begin{aligned} e_k(x_1, r_1)\, e_k(x_2, r_2) &= (\alpha^{r1} \bmod p,\, \alpha^{x1}\, \beta^{r1} \bmod p)(\alpha^{r2} \bmod p,\, \alpha^{x2}\, \beta^{r2} \bmod p) \\ &= (\alpha^{r1+r2} \bmod p,\, \alpha^{x1+x2}\, \beta^{r1+r2}) \bmod p \\ &= e_k(x_{1+} x_2,\, r_{2+} r_2) \end{aligned}$$

4.6 MD5 Algorithm

MD5 is used to verify the content of the message it is a message authentication protocol. It is essentially a hashing; a mapping from a random text to a fix bit string of length 128 bit. Earlier schemes (say RSA) used for encryption/decryption and digital signatures has put a heavier processing load on applications. Recently, a competing system has begun to challenge ie; elliptic curve cryptography. ECC offers equal security for a far smaller key size and hence reducing processing overhead. Our proposed scheme use MD5 because of following reasons:

1. Key length of MD5 is comparatively less. MD5 uses key length of 64 to 512 bits.
2. Block size of MD5 is 128 bits.
3. MD5 is even faster on 32 bit machines.
4. Strong against Digital Certificates.

Step 1: Append Padded Bits i.e. the message is padded so that its length is congruent to 448, modulo 512. A single bit i.e. "1" is appended and then "0" bits are appended so that length equals 448 modulo 512.
Step 2: Append Length i.e. 64 bit representation of message is appended to result of step1 and resulting message has length that is exact multiple of 512.
Step 3: Initialize MD buffer i.e. a 4-word buffer (A,B,C,D) is used to compute Message Digest where A,B,C,D is 32 bit register. These registers are initialized to hexadecimal values.
Step 4: Process message in 16 word block.
Step 5: Output is obtained.

5. Results and Analysis

Diffie-Hellman Key Transactions is one of additional accepted and interesting methods of key distribution. It is a public-key cryptographic scheme whose merely intention is for allocating keys. Purpose of the Diffie Hellman is to allow two users to securely transactions a key that can after that be utilized for subsequent encryption of messages.

5.1 Cloud integration verification

The content of outsourced data can be confirmed by whichever client and TPA. This is completed via invigorating server by providing a little folder and block randomly. Up on examination, cloud storage server computes origin hash agenda for consented file and blocks and next returns computed origin hash plan and early stored hash plan alongside signature. Next TPA and client uses district key and confidential key in arrange to decrypt gratified and difference origin hash agenda alongside origin hash plan returned by customers.

Chart-1: Total Integrity errors given the iterations

It is clear from above chart and table that out proposed integrity scheme produces minimum errors on average less than **1 error per Million Client Requests.**

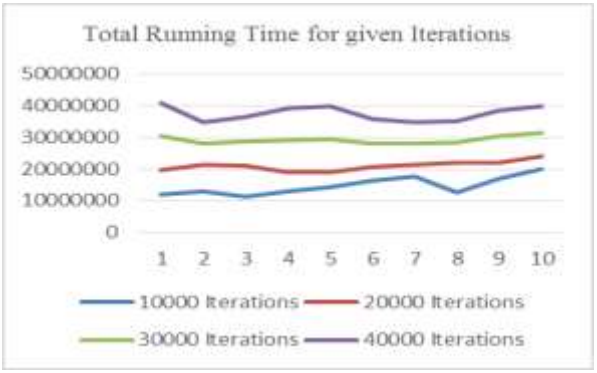

Chart-2: Line chart showing Total Running time for Cloud KeyGen and Checking Integrity Proofs, Indicates that the algorithm is linearly scalable

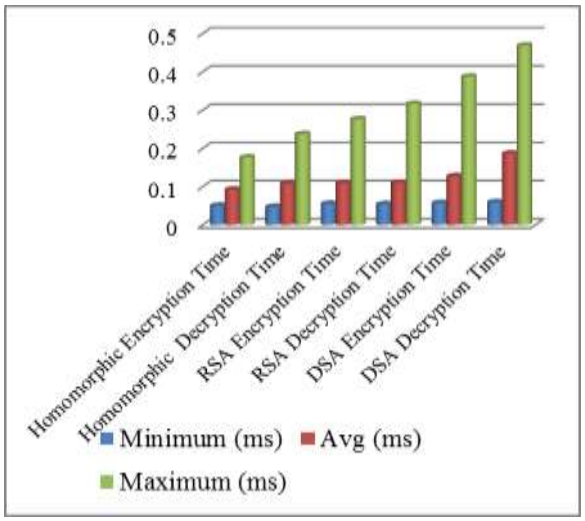

Chart-3: Encryption and Decryption Time of Various Encryption Algorithms

6. Conclusion

In cloud, there are countless gains to release burden of data association for user, such as facile to entrance, cheap storage space, convenient resource-sharing. Users usually upload data to cloud storage space servers, next delete innate copies. So users capitulated finished manipulation above data itself. After users confided their data to cloud storage, most concern setback is that cloud ability supplier (CPS) could delete users' data and tamper alongside users' data maliciously. For sake of hobby, CPS has countless motivations to flounder obligation of protecting user data. Such as CPSs in arrange to save their own storage space save working expenses, CPS delete data that users admission little; contraption obligation lead to defeat of data, CPS obscure data beat event; unintentionally delete user data after transfer data to new storage servers. In this work, we have given design and implementation of Homographic system for verifying integrity of multi-tenant cloud infrastructures. Our scheme was industrialized to cut computational and storage overhead of client as well as to minimize computational overhead of the cloud storage server. Our system produces minimum errors on average less than 1 error every Million Appeal.

7. Future Works

There is a number of attractive Homomorphic variants to discover in future up work. The protocols we have delineated above for Homomorphic merely furnish assurance for static files. We are investigating in their work mean of comparable protocols that accommodate file updates. We trust that Homomorphic methods we have gave in this work aid pave the way for priceless behavior to Cloud file arrangement potential and Integrity. We can additionally work on

1. Applications of completely homomorphic encryption IaaS
2. Environments Non-malleability and homomorphic encryption
3. Fully homomorphic encryption and functional decryption

Another vital open question relates to assumptions underlying current fully homomorphic encryption systems. All recognized fully homomorphic encryption schemes are established on hardness of lattice problems. The usual question that arises can we craft fully homomorphic from supplementary ways – say, for example, from number-theoretic assumptions? Can we hold in subject of hardness of factoring and discrete logarithms in this problem?

8. REFERENCES

1. Yubin Yang; Hui Lin; Jixi Jiang,"Cloud analysis by modeling the integration of heterogeneous satellite data and imaging",IEEE,Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 2006
2. Kaewpuang, R.; Uthayopas, P.; Srimool, G.; Pichitlamkhen, J.,"Building a Service Oriented Cloud Computing Infrastructure Using Microsoft CCR/DSS System",IEEE,Computer Sciences and Convergence Information Technology, 2009. ICCIT '09. Fourth International Conference on, 2009
3. Tao Wu; Kun Qin,"Inducing Uncertain Decision Tree via Cloud Model",IEEE,Semantics, Knowledge and Grid, 2009. SKG 2009. Fifth International Conference on, 2009
4. Yi Zhao; WenlongHuang,"Adaptive Distributed Load Balancing Algorithm Based on Live Migration of Virtual Machines in Cloud",IEEE,INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on, 2009
5. Zhifeng Xiao, Yang Xiao, "Security and Privacy in Cloud Computing", Dept. of Comput. Sci., Univ. of Alabama, Tuscaloosa, AL, USA, 10.1109/SURV.2012.060912.00182, 843-859, 2013
6. Schiffman, J., Yuqiong Sun, Vijayakumar, H., Jaeger, T., "Cloud Verifier: Verifiable Auditing Service for IaaS Clouds", , 10.1109/SERVICES.2013.37, 239-246, 2013
7. Alabool, H.M., Mahmood, A.K., "Common Trust Criteria For IaaS cloud evaluation and selection", Dept. Comput. & Inf. Sci., Univ. Teknol. Petronas, Tronoh, Malaysia, 10.1109/ICCOINS.2014.6868444, 1-6, 2014
8. Hazarika, P., Baliga, V., Tolety, S., "The mobile-cloud computing (MCC) roadblocks", Siemens Technol. & Services, Bangalore, India, 10.1109/WOCN.2014.6923101, 1-5, 2014
9. Selvakumar, C., Rathanam, G.J., Sumalatha, M.R., "PDDS - Improving cloud data storage security using data partitioning technique", Dept. of Inf. Technol., Anna Univ., Chennai, India, 10.1109/IAdCC.2013.6506806, 7-11, 2013