Secure Cloud Computing with RC4 Encryption and Attack Detection Mechanism

Laxmikant Mishra
M.Tech Research Scholar
Computer Science
Gyan Ganga Institute of Technology &
Management Bhopal

Amit Sharma
Assistant Professor
Computer Science
Gyan Ganga Institute of Technology &
Management Bhopal

ABSTRACT

The growing requirement of system resources, memory requirement and huge space etc. have sprinted up the demand of cloud computing. The ease in the use and dynamic demand completion nature will also make it a future business platform. But we cannot forget the second side of the coin as the ease will comes with some negative cost. By the growing demand huge amount of data has been uploaded, update and shared. But data sharing and updating in the cloud environment may be risky. There are some trust mechanism should be there to secure the data. Our paper main motivation is to secure the sharing environment by sharing the data by the use of RC4 encryption and decryption mechanism. Then we have also detected the unauthorized data connection if there by our dynamic attack alert system.

Keywords

Cloud Computing, RC4, Security, Attack Alert.

1. INTRODUCTION

Cloud computing provide on demand resources based on pool of assets accessible by the cloud suppliers [1][2][3]. From the part of customary registering the preferences of distributed computing are: nimbleness, lower section cost, gadget independency, area independency, and adaptability [4][5]. At the same time the security concerns are the real key perspectives later on distributed computing period. There are a few security majors are exhibited in [6], [7], [8],[9],[10],[5].Virtualization, superior registering are additionally the more prominent office parts of distributed computing. Be that as it may to attain to the execution on the parallel framework and keeping up the respectability is extreme [11]. In all these works, extraordinary endeavors are made to outline arrangements that meet different necessities: high plan effectiveness, stateless check, unbounded utilization of inquiries and hopelessness of information, and so on. Considering the part of the verifier in the model, all the plans exhibited before fall into two classifications: private auditability and open auditability [5]. Despite the fact that plans with private auditability can accomplish the plans effectively, yet it is testing circumstance if the information is putting away secretly [5]. Virtualization is the key highlight of distributed computing. By which information imparting is conceivable between diverse machines of virtual presence from the server farm [12]. Virtualization empowers the live movement [9] of virtual machines (i.e. migrating a VM starting with one host then onto the next without bringing it down) which helps in keeping up the guaranteed SLA to the cloud computing [12].

The cloud computing structure depends on the layers for information transportation. The three fundamental administration layers that involve the distributed computing structural engineering in view of which the on interest administration will be provided [13]. As per [13] Software as a Service (SaaS) has changed desktop-based programming applications into online programming items that can be utilized around the world. A generally utilized application is Salesforce.com, a client relationship administration (CRM) programming for communicating with organizations and clients [13]. As indicated by [13] Platform as a Service (PaaS) is a situation for Cloud Computing Security Management for creating and building applications for diverse situations. As indicated by Infrastructure as a Service (IaaS) generally includes virtualization situations as acquired administrations instead of physical or devoted PC gear. The primary advantage of this kind of framework is there is no need of intense work station as the client area yet on interest assets/programming can impart it to lease. So on the off chance that it is coordinated with the security administrations it gets to be capable. Information mining errand can be figured in cloud environment for legitimate information arrangement and order [14]. Give secure system to giving portable distributed computing making information get to and taking care of instrument by information mining [15].

2. LITERATURE SURVEY

In 2010, Chenguang Wang et al. [16] propose supporting investigation of a system to tackle distributed computing security issue with private face distinguishment. The technique has three sections: client part gives face pictures; cloud instatement part has a face subspace and formats database; cloud private coordinating ID part contains the center calculation of the system, looking at two scrambled numbers under twofold encoded conditions. The exploratory results demonstrate the strategy can guarantee that cloud neither know client's genuine face information, nor the face private coordinating ID result, to make client's face information secure, we add to a valid, productive, low-complex system to ensure distributed computing security. In 2011, Ling Zheng et al. [17] contrasting private cloud and open cloud , records contrasts in the middle of them and advances a structural engineering of private distributed computing to bolster keen brace, elucidates structure of every layer, and presents idea of private distributed computing working framework and system virtualization. It gives the hypothetical reference to assemble the private distributed computing, accordingly advances the development of the savvy matrix. In 2011, Ming Li et al. [18] introduced a contextual investigation utilizing online Personal Health Record (PHR), they first demonstrate the need of hunt ability approval that decreases the security introduction coming about because of the indexed lists, and build an adaptable structure for Authorized Private Keyword Search (APKS) over encoded cloud information. They then propose two novel answers for APKS in view of a late cryptographic primitive, Hierarchical Predicate Encryption (HPE). Their answers empower proficient multi-dimensional watchword looks with extent inquiry; permit appointment and repudiation of hunt abilities. They improve the inquiry protection which conceals clients' question decisive words against the server. In 2011, Yanjiang Yang et al. [19] recommend that Storage-as-an administration is a key part of the distributed computing foundation. Database outsourcing is a normal utilization situation of the distributed storage administrations, wherein information encryption is a decent approach empowering the information manager to hold its control over the outsourced information. Searchable encryption is a cryptographic primitive taking into account private decisive word based inquiry over the scrambled database. The setting of big business outsourcing database to the cloud requires multi-client searchable encryption, though practically all current plans consider the single-client setting. To extension this crevice, they propose a viable multi-client searchable encryption plan, which has various points of interest over the known methodologies. In 2011, Wang et al. [20] recommended that distributed computing has been imagined as the cutting edge building design of IT Enterprise. It moves the application programming and databases to the brought together vast server farms, where the administration of the information and administrations may not be completely dependable. The issue of guaranteeing the trustworthiness of information stockpiling in Cloud Computing. Specifically, they consider the assignment of permitting an outsider evaluator (TPA), for the cloud customer, to check the trustworthiness of the element information put away in the cloud. The presentation of TPA disposes of the association of the customer through the reviewing of whether his information put away in the cloud is undoubtedly in place, which can be critical in accomplishing economies of scale for Cloud Computing. The similar types of work are also presented in [21-25]. In 2012, Syed Naqvi et al. [26] present a formal method for testing the effect of versatility and heterogeneity on the united Cloud security administrations. Their means to add to a mean of evaluating the effect on security works under different working conditions and parameters of unified Cloud organizations. Their consequences of this work will help organizations to recognize the best security structural planning that will fit their Cloud architectures and execution prerequisites. In 2012, Huaglory Tianfield et al. [27] presents a thorough study on the difficulties and issues of security in distributed computing. They first investigate the effects of the unmistakable qualities of distributed computing, to be specific, multi-occupancy, flexibility and outsider control, upon the security prerequisites. At that point, they examine the cloud security necessities as far as the crucial issues, i.e., privacy, honesty, accessibility, trust, and review and agreeability. They talk about the scientific categorization for security issues in distributed computing. They compress the security issues in distributed computing by cloud security structural planning. In 2012, Abdullah Abuhussein et al. [28] propose Healthcare, training, business, and numerous different areas take a gander at distributed computing as an attempt to tackle the persistent deficiency in volume, base, availability, and observing strength. Be that as it may, moving information to the cloud infers moving control of the client's information to the cloud administration supplier inconclusively. Subsequently, the security and protection of the client's data turns into a critical issue. Evaluating and looking at among potential distributed computing administrations, represents an issue for learner clients intrigued to move their work to the cloud to pick security choices that are sufficient and powerful in the meantime. They endeavors to distinguish and classify a rundown of properties which mirror the different parts of cloud security and protection. These ascribes can be utilized to evaluate and think about distributed computing administrations so shoppers can settle on knowledgeable decisions. Cloud administration suppliers can utilize them to construct and/or offer better cloud arrangements. In 2012, Wentao Liu et al. [29] propose that the security issue of distributed computing is vital and it can keep the fast improvement of distributed computing. It presents some distributed computing frameworks and examines distributed computing security issue and its system as per the distributed computing ideas and characters. The information protection and administration accessibility in distributed computing are the key security issue. Single security technique can't tackle the distributed computing security issue and numerous customary and new advancements and procedures must be utilized together for ensuring the aggregate distributed computing framework. In 2013, Nikhilesh Pant et al. [30] present the approachs for cloud reception and cloud security appraisal to investigate potential security and consistence suggestions in cloud environment. They examines in point of interest on how an association may move ahead for security and agreeability evaluation amid the cloud processing. Their methodology and ideas itemized in this paper would be helpful for associations that are included in the cloud selection process. In 2013, Du meng et al. [31] examines distributed computing information security issues, including tile security of information transmission, stockpiling, security and administration of security. Concentrate on widespread information administration influence cloud security examination, and brought up that an achievement in the advancement of this distributed computing, attempt to identify the comparing methods and long haul improvement bearing. In 2013, Fan Yang et al. [32] proposed that the information security and protection on cloud is an essential issue, turning into the greatest hindrance of distributed computing advancement. A Trusted Cloud Computing Platfom (TCCP) in light of remote authentication construct a trusted cloud for inhabitant.

3. PROPOSED WORK

We have constructed the cloud virtualization mechanism in JSP based environment by using Net beans tool. We have developed a cloud provider based on 4 different servers. These server have different resource capabilities based on the capacities data has been uploaded. For this the user should have to register in the cloud environment. After submitting the details the user will register in this environment. So the authentication process has been completed and the user is eligible to select the server and able to upload the data. The whole procedure is shown in figure 1.

In the proposed approach a register user in the cloud can establish a secure connection with the cloud for gathering the appropriate data file which they needs from the servers as specified above. To ensure this, the user must be authorized in the cloud database. After authorization, the user in the cloud can request only supported files from the server. So the authentication process has been completed and the user is eligible to select the server and able to upload the data. If need be then the cloud user can request the fata from another user in the cloud from the listed servers. So that data can be shared. After the cloud user requests the desire file from the listed server for required data file, cloud framework automated this process and prepares the data for secure data transaction. In this data transaction we have applied RC4 encryption technique for encryption and decryption. The process mode for data preparation is basically automated so that the process time is very less. Then the cloud framework starts the data preparation by using RC4 algorithm and generated the decryption key. The security of this encryption thought relies on upon the last clients to watch the key suitably. In the event that an unlawful client were able to catch the key, they would have the capacity to inspect and record the encoded reports. We are additionally dynamism the information presence component and also the arbitrary and variable key security.

The above procedure is the first way to handle the data security in the cloud environment as the receiver of the data should use proper decryption key to achieve the data. Without this the data will not be discovered in the future. The second mechanism we have adopted in the direction of detection. As all the users are registered in the cloud and there user id is unique in the database. So by the use of use rid our program can check the receiving data listening. If the data is being listened by the same cloud user then it reply with 1 ort true or it return the value 0 or false. By this means we will be able to detect the response from the receiver. In this way we will also able to detect any unwanted activity will cause in the near future and prevent it or resend the data. As not any protection level can protect the system 100 % so the detection technique will assure in this regards.

Proposed Algorithm

This algorithm is proposed for the process of the file transfer by the server.

```
1)  Inputs: The set of Input Files ($IF_1$, $IF_2$……….$IF_n$) from
    the full set of request by the client user.
2)  Output: Process File by the Server ($PF_1$, $PF_2$
    ………..$PF_n$).
3)  do
        Find the peak request from the file request set.
        Design a sequence of file request loads
        ($fr_1$,$fr_2$……$fr_n$) to search the Global File request.
        For each request loads(FR= $fr_1$, $fr_2$……$fr_n$)
        Input:
        User-supplied b byte key preloaded into the c-
        word[31]
          array L[0,…, c - 1]
          Number r of rounds
          Pw = Odd((e – 2)2w)
          Qw = Odd((ø – 1)2w)
        Output:
          w-bit round keys S[0,…, 2r + 3]
        Procedure:
          S[0] = Pw
          for i = 1 to (2r + 3) do
            S[i] = S[i _ 1] + Qw
          A = B = i = j = 0
          v = 3 x max{c, 2r + 4}
          for s = 1 to v do
          {
            A = S[i] = (S[i] + A + B) <<< 3
            B = L[j] = (L[j] + A + B) <<< (A + B)
            i = (i + 1) mod (2r + 4)
            j = (j + 1) mod c
  }
Partition;
 End;
4)  Send data to the client with relevant log file and also
    maintain a log report for this event.
5)  Finish.
```

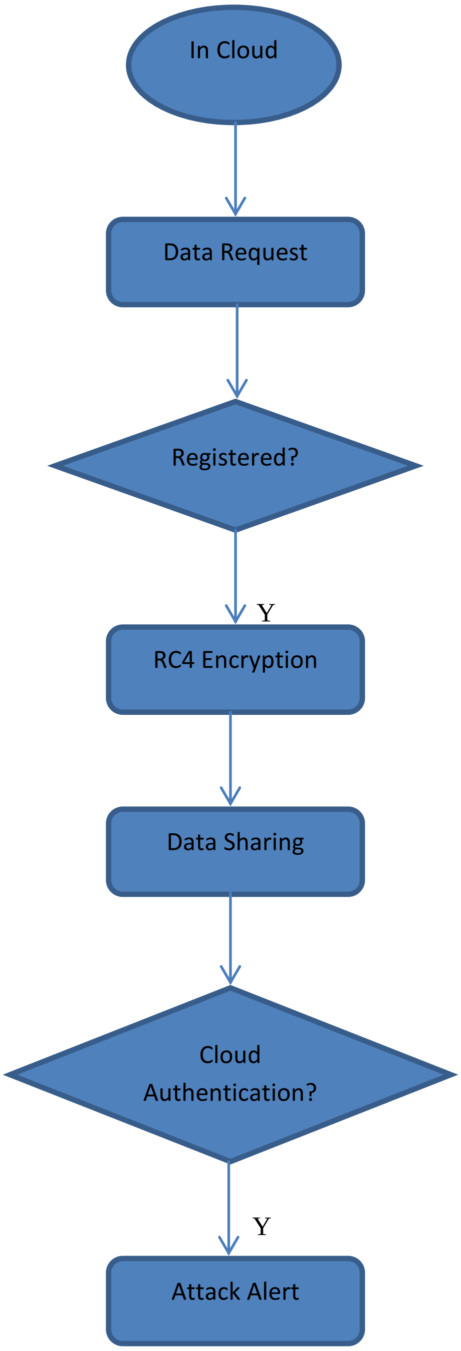

Figure 1: Flowchart

4. RESULTS

The result shown by our methodology has been proved better. As from table 1, the data report shown shows the random behavior of password which significant improves the security as the password is random so the attack will not be easy in the future trends. The encryption size and decryption size is same so there is no data loss in case of textual data. Encryption decryption time is also less. The difference suggested in table 2 is also minimum which shows the significant improvement in the alert system.

Table 1: Data Report Status

Filename	Server name	Upload date	Open	Password	Status	EncS	DecS	EncryT	DecryT
Iphone.txt	server2	Sun Mar 29 17:03:43 IST 2015	yes	oE9Nj8y7	safe	1668	0	0	0
assddd.doc	server2	Sun Mar 29 17:07:32 IST 2015	yes	hP3Sk6n9	safe	23040	0	0	0
demoi.txt	server2	Sun Mar 29 18:05:36 IST 2015	yes	qR7Cw8l9	safe	555	0	0	0
demoi.txt	server4	Sun Mar 29 18:06:41 IST 2015	yes	qR7Cw8l9	safe	555	555	0	0
assddd.doc	server3	Sun Mar 29 18:10:43 IST 2015	yes	wE2Ni1m5	safe	23040	0	0	0
Iphone.txt	server4	Thu Apr 02 21:53:15 IST 2015	yes	oE9Nj8y7	safe	1668	1668	16	0
assddd.doc	server4	Thu Apr 02 22:01:43 IST 2015	yes	wE2Ni1m5	safe	23040	23040	16	11
demoi.txt	server4	Sun Apr 05 17:31:52 IST 2015	no	qR7Cw8l9	attack	555	555	16	0
assddd.doc	server4	Sun Apr 05 19:04:55 IST 2015	yes	wE2Ni1m5	safe	23040	23040	113	9

Table 2: attack Report Status

Filename	Attack time	Alert time	difference
demoi.txt	Tue Mar 31 21:31:16 IST 2015	Tue Mar 31 21:31:16 IST 2015	26
demoi.txt	Thu Apr 02 22:19:29 IST 2015	Thu Apr 02 22:19:29 IST 2015	30
demoi.txt	Sun Apr 05 19:14:44 IST 2015	Sun Apr 05 19:14:44 IST 2015	6

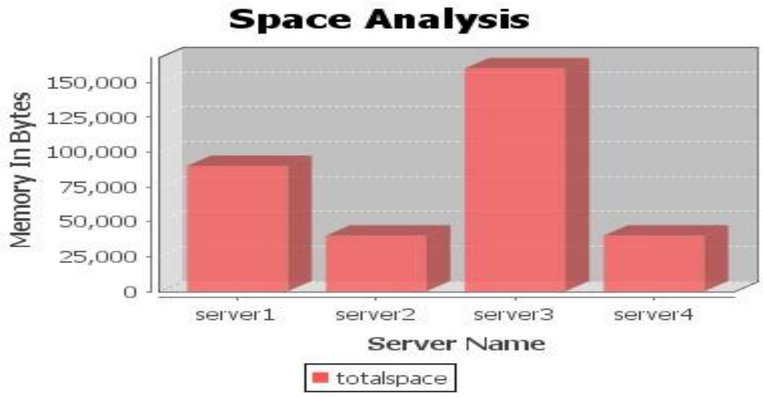

Figure 2: Space Analysis

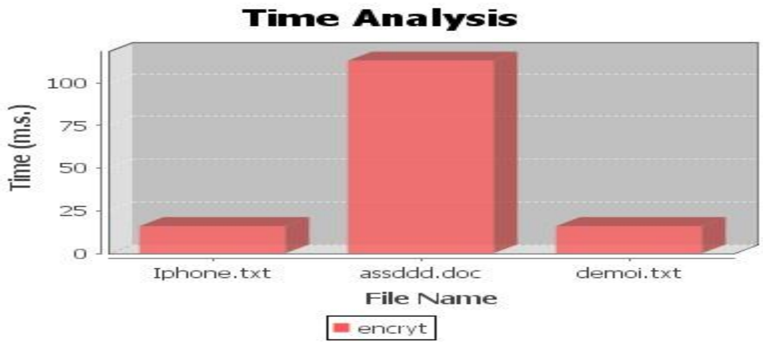

Figure 3: Time Analysis

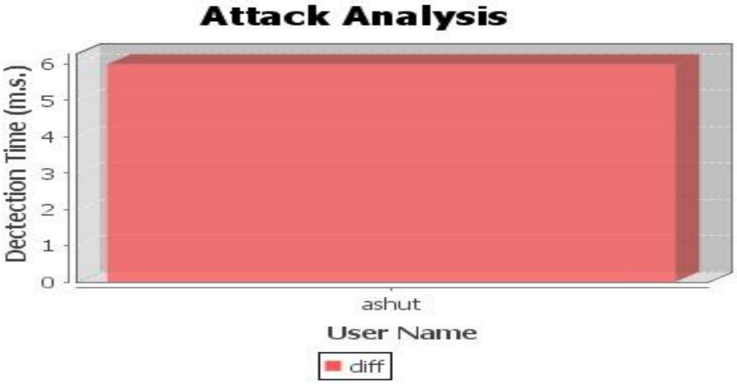

Figure 4: Attack Analysis

5. CONCLUSION

This paper has been suggested an improved and efficient way of data security. It provides the betterment in encryption and decryption with proper key randomization with RC4 algorithm. Our approach provides a better information security with no loss as well as alert system is there which will provide a timely alert. The size and data management of the framework is also improved by the centric control.

6. REFERENCES

[1] MM. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[2] Igor Ruiz-Agundez, Yoseba K. Penya and Pablo G. Bringas, “Cloud Computing Services Accounting”, International Journal of Advanced Computer Research (IJACR) ,Volume 2, Number 2, June 2012.

[3] Ajey Singh, Maneesh Shrivastava, “Overview of Security issues in Cloud Computing”, International Journal of Advanced Computer Research (IJACR) Volume 2,Number 1,March 2012.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.

[5] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava,” Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment”, CONSEG-2012.

[6] A. Juels and B.S. Kaliski Jr., “Pors: Proofs of Retrievability for Large Files,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 584-597, 2007.

[7] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. 14th Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’08), pp. 90-107, 2008.

[8] K.D. Bowers, A. Juels, and A. Oprea, “Proofs of Retrievability: Theory and Implementation,” Report 2008/175, Cryptology ePrint Archive, 2008.

[9] M. Naor and G.N. Rothblum, “The Complexity of Online Memory Checking,” Proc. 46th Ann. IEEE Symp. Foundations of Computer Science (FOCS ’05), pp. 573-584, 2005.

[10] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya , “Service-Oriented Cloud Computing Architecture” , 2010 Seventh International Conference on Information Technology.

[11] G K Patra, Nilotpal Chakraborty,” Securing Cloud Infrastructure for High Performance Scientific Computations Using Cryptographic Techniques”, International Journal of Advanced Computer Research (IJACR) ,Volume-4 Number-1 Issue-14 March-2014.

[12] Nilesh Pachorkar, Rajesh Ingle,” Multi-dimensional Affinity Aware VM Placement Algorithm in Cloud Computing”, International Journal of Advanced Computer Research (IJACR) Volume-3 Number-4 Issue-13 December-2013.

[13] Tschinkel, Brian. "Cloud Computing Security Understanding Risk Areas & Management Techniques." (2011).

[14] Ashutosh Kumar Dubey, Animesh Kumar Dubey,Vipul Agarwal, Yogeshver Khandagre, “Knowledge Discovery with a Subset-Superset Approach for Mining Heterogeneous Data with Dynamic Support”,Conseg-2012.

[15] Ashutosh K. Dubey, Ganesh Raj Kushwaha and Nishant Shrivastava,‖ Heterogeneous Data Mining Environment Based on DAM for Mobile Computing Environments, Information Technology and Mobile Communication Communications in Computer and Information Science, 2011, Springer LNCS.

[16] Chenguang Wang, Huaizhi Yan,” Study of Cloud Computing Security Based on Private Face Recognition”,IEEE 2010.

[17] Ling Zheng, Yanxiang Hu,Chaoran Yang,” Design and research on private cloud computing architecture to Support Smart Grid”, Third International Conference on Intelligent Human-Machine Systems and Cybernetics, 2011.

[18] Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou,” Authorized Private Keyword Search over Encrypted Data in Cloud Computing”, 31st International Conference on Distributed Computing Systems, 2011.

[19] Yanjiang Yang,” Towards Multi-User Private Keyword Search for Cloud Computing”, IEEE 4th International Conference on Cloud Computing, 2011.

[20] Wang, Qian, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. "Enabling public auditability and data dynamics for storage security in cloud computing." Parallel and Distributed Systems, IEEE Transactions on 22, no. 5 (2011): 847-859.

[21] Nilesh Pachorkar and Rajesh Ingle, " Affinity Aware VM Colocation Mechanism for Cloud " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-17, December-2014 ,pp.956-960.

[22] Surya Prabha.U.S, Marikkannu.P, Arul Vineeth.A.D, " Ciphertext Policy Attribute Set Based Encryption with One-Fold Data Access in Cloud " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-14, March-2014 ,pp.110-115.

[23] Pritam Fulsoundar, Rajesh Ingle, " Prediction of Performance Degradation in Cloud Computing " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-13, December-2013 ,pp.126-129.

[24] Sampada Kembhavi and Gajendra Singh, " Auto Upload and Chi-Square Test on Application Software as a Service for Cloud Computing Environment " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014 ,pp.26-31.

[25] Sampada Kembhavi, Ravindra Gupta, Gajendra Singh, " An Efficient Algorithm for Auto Upload and Chi-Square Test on Application Software " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-10, June-2013 ,pp.121-125.

[26] Naqvi, S.; Michot, A.; Van de Borne, M., "Analysing Impact of Scalability and Heterogeneity on the Performance of Federated Cloud Security," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on , vol., no., pp.1137,1142, 25-27 June 2012.

[27] Tianfield, H., "Security issues in cloud computing," Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on , vol., no., pp.1082,1089, 14-17 Oct. 2012.

[28] Abuhussein, A.; Bedi, H.; Shiva, S., "Evaluating security and privacy in cloud computing services: A Stakeholder's perspective," Internet Technology And Secured Transactions, 2012 International Conference for, vol., no., pp.388,395, 10-12 Dec. 2012.

[29] Wentao Liu, "Research on cloud computing security problem and strategy," Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on , vol., no., pp.1216,1219, 21-23 April 2012.

[30] Pant, N.; Parappa, S., "Seeding the cloud in a secured way: Cloud adoption and security compliance assessment methodologies," Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on, vol., no., pp.305, 308, 23-25 May 2013.

[31] Du meng,” Data security in cloud computing”, The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka.

[32] Fan Yang; Li Pan; Muzhou Xiong; Shanyu Tang, "Establishment of Security Levels in Trusted Cloud Computing Platforms," Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing , vol., no., pp.2119,2122, 20-23 Aug. 2013.