Cloud Computing Security: A Survey

Sheetal Mahalle
M. Tech Student, Computer Science
TIT Bhopal

Ranjeet Jaiswal
Professor, Computer Science
TIT Bhopal

ABSTRACT
Due to volume output, easy access of information, less time more work to be done, virtualization technique and pay per use increase the use of cloud computing in today's era. It may be used in all the area including Social websites, E-Commerce, Education and heavy data warehouse system. The on demand remote capacity makes it the first reason to choose cloud service. Now several companies are choosing the services of cloud computing. Then the question of security of the cloud data may arise. As the data on the cloud computing should be secure. In this paper a study has been made in the direction of cloud computing security. Based on the study some new insights has been gathered and suggested.

Keywords
Cloud Computing, Virtualization, Security, E-commerce

1. INTRODUCTION
From the part of customary registering the favorable circumstances of distributed computing are: readiness, lower section cost, gadget independency, area independency, and versatility. Yet the security concerns are the significant key angles later on distributed computing period. There are a few security majors are exhibited in [1].Virtualization, elite figuring are additionally the more prominent office parts of distributed computing. In any case to accomplish the execution on the parallel framework and keeping up the trustworthiness is extreme [2]. In all these works, extraordinary endeavors are made to outline arrangements that meet different prerequisites: high plan proficiency, 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 introduced before fall into two classes: private auditability and open auditability. In spite of the fact that plans with private auditability can attain to the plans effectively, yet it is testing circumstance if the information is putting away secretly. Virtualization is the key peculiarity of distributed computing by which information imparting is conceivable between distinctive machines of virtual presence from the server farm [3]. Virtualization empowers the live movement of virtual machines (i.e. moving 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 purchaser furthermore for adjusting load crosswise over physical servers in the information centers[3]. It can be used in the respect of university enterprises also. The need of security in cloud computing has been increased due to the wide3acceptability of cloud computing in different area. The different areas can be find from the research presented in [3][4][5][6][7][8][9].

The main cloud providers are Google,Microsoft, Salesforce.com, Vmforce.com and Amazon etc. The cloud computing system depends on the layers for information transportation. The three principle administration layers that involve the distributed computing building design in light of which the on interest administration will be provided. As per 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 connecting with organizations and clients. As indicated by Platform as a Service (PaaS) is a domain for Cloud Computing Security Management for creating and building applications for diverse situations. As per Infrastructure as a Service (IaaS) basically includes virtualization situations as bought administrations as opposed to physical or committed PC gear. The layers are demonstrated in figure 1. The uses of cloud computing is clear from figure 2.

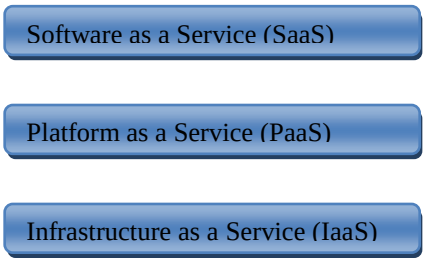

Figure 1: Types of Service Models [14]

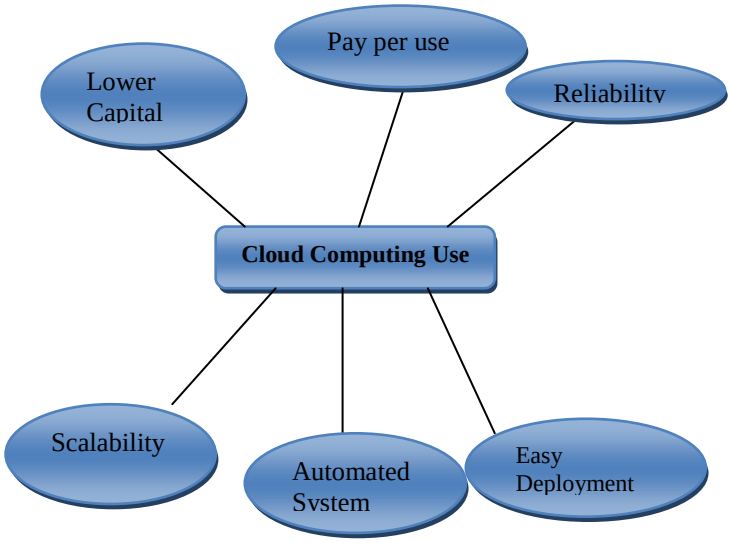

Figure 2: Cloud Computing Use

Cloud computing provides power and flexibility in computing but security is the major concern. Our main motivation of this paper is to find out better methodology to provide good security system in cloud computing data sharing.

2. LITERATURE SURVEY
In 2012, Huaglory Tianfield et al. [10] presents a complete study on the difficulties and issues of security in distributed computing. They first investigate the effects of the unique attributes of distributed computing, specifically, multi-tenure, versatility and outsider control, upon the security necessities. At that point, they dissect the cloud security

necessities regarding the central issues, i.e., privacy, uprightness, accessibility, trust, and review and agreeability. They talk about the scientific categorization for security issues in distributed computing. They abridge the security issues in distributed computing by cloud security building design.

In 2012, Abdullah Abuhussein et al. [11] recommend Healthcare, instruction, business, and numerous different areas take a gander at distributed computing as an attempt to illuminate the ceaseless lack in volume, framework, availability, and checking intensity. Then again, moving information to the cloud suggests 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 vital issue. Evaluating and contrasting among potential distributed computing administrations, represents an issue for beginner clients intrigued to move their work to the cloud to pick security alternatives that are sufficient and powerful in the meantime. They endeavor to recognize and order a rundown of qualities which mirror the different parts of cloud security and protection. These ascribes can be utilized to survey and think about distributed computing administrations so buyers can settle on accomplished decisions. Cloud administration suppliers can utilize them to fabricate and/or offer better cloud arrangements.

In 2012, Wentao Liu et al. [12] recommend that the security issue of distributed computing is essential and it can keep the fast advancement of distributed computing. It presents some distributed computing frameworks and dissects distributed computing security issue and its method as per the distributed computing ideas and characters. The information protection and administration accessibility in distributed computing are the key security issue. Single security system can't take care of the distributed computing security issue and numerous conventional and new innovations and techniques must be utilized together for securing the aggregate distributed computing framework. The security system with different techniques are also suggested in [13][14][15].

In 2013, Nikhilesh Pant et al. [16] present the techniques for cloud appropriation and cloud security evaluation to investigate potential security and agreeability suggestions in cloud environment. They examines in subtle element on how an association may continue for security and agreeability appraisal amid the cloud reckoning. Their methodology and ideas point by point in this paper would be helpful for associations that are included in the cloud selection process.

In 2013, Du meng et al. [17] examines distributed computing information security issues, including tile security of information transmission, stockpiling, security and administration of security. Concentrate on general information administration influence cloud security investigation, and called attention to that a leap forward in the advancement of this distributed computing, attempt to identify the relating systems and long haul improvement bearing.

In 2013, Fan Yang et al. [18] proposed that the information security and protection on cloud is an essential issue, turning into the greatest boundary of distributed computing improvement. A Trusted Cloud Computing Platfom (TCCP) taking into account remote confirmation assemble a trusted cloud for inhabitant. The basic segment is incorporated Trusted Coordinator, taking the spot of occupants to confirm hubs exclusively in distributed computing stage. Be that as it may, when a considerable measure of occupants request hubs in the meantime, Trusted Coordinator (TC) perhaps can't manage these solicitations rapidly .To address this issue, they propose the foundation of security-level for distinctive applications in TCCPs, which partitions Trusted Coordinator into three, every in charge of verifying diverse application kind. The diverse verification approaches, for example, client watchword correlation, picture hash confirmation and trusted chain estimation, as indicated by distinctive security levels.

In 2013, Issa M. Khalil et al. [19] recommend that the Security issue in distributed computing is indicated to be the greatest impediment that could subvert the wide profits of distributed computing. The new ideas that the cloud presents, for example, multi-tenure, makes new difficulties to the security group. Tending to these difficulties requires, notwithstanding the capacity to develop and tune the efforts to establish safety created for different frameworks, proposing new security arrangements, models, and conventions to address the novel cloud security challenges. They give far reaching investigation of distributed computing security that incorporates grouping of known security dangers and the best in class rehearses in the try to balance these dangers. They likewise gives the reliance level inside arrangement and gives an answer in manifestation of preventive activities as opposed to proactive activities. The classification approach is also suggested in [20].

In 2013, Azzedine Benameur et al. [21] recommend that that the distributed computing standard for expansive scale bases and more military and basic base frameworks are moving towards cloud stages too. Utilizing the cloud can lessen the aggregate expense of possession and apportions assets on interest so as to adapt to load. Two key desires when moving to cloud-based administrations are accessibility and security. Then again, late blackouts with significant Platform as a Service (PaaS) suppliers allegedly generally in the press have demonstrated that even a cloud stage can't give immaculate accessibility. Furthermore, a 2013 Defense Science Board write about "Digital Security and Reliability in a Digital Cloud" finds that while some security practices can be enhanced in a cloud domain, a few dangers are distinctive or exacerbated. They display a way to influence the flexibility and on-interest provisioning gimmicks of the cloud to enhance strength to accessibility concerns and regular assaults. Their methodology uses broadening of lightweight virtualized application servers for excess and assurance against both application mistakes and system based assaults.

In 2013, Liu Xiao-hui et al. [22] recommend Cloud registering gets to be more natural to individuals, and its application field gets to be more generally. They presented its improvement status and analysized the security issues. Advanced a few trains of considered the security, and recommended that trusted distributed computing will be a guaranteeing bearing without bounds cloud security scrutinizes.

3. PROBLEM DOMAIN

Cloud registering is being received at a fast rate in light of the fact that it has an expansive number of upsides for a wide range of organizations and builds effectiveness. Ventures are diminishing stockpiling expenses by utilizing online stockpiling arrangement suppliers. This permits the endeavour to store enormous measures of information on outsider servers. One of the real points of interest is that the stockpiling limit is versatile and therefore, the undertaking pays for the measure of capacity that it needs. Moreover, access to the information is accessible through any Internet association. Versatility and allotment of assets are the real

points of interest of virtualization. Virtualization permits chairmen to utilize transforming power all the more productively and offer assets crosswise over equipment gadgets by adjusting multi-inhabitant clients. Overseers can raise virtual machines (VMs) and servers rapidly without having the overhead of requesting or provisioning new equipment. Equipment assets that are no more needed for an administration or application can be re-relegated rapidly and additional preparing force can be devoured by different administrations for greatest productivity. By utilizing all the accessible handling power and untethering the equipment from a solitary server model, cost efficiencies are acknowledged in both private and open mists. Though the presentation of distributed computing is in no way, shape or form the first innovation movement to cause significant security concerns, it is a noteworthy point of reference. As of not long ago, most associations have put away and dealt with their most basic data resources in physically divided server farms either all alone premises or inside leased pens everywhere facilitating suppliers. So information driven security is required. Minimizing the information security dangers, while moving and putting away information, was simpler for associations to control inside private server farms than inside the cloud. Putting away information in the cloud implies that information will be mixed on imparted servers. On the off chance that organizations jump into cloud without considering the unintended results, basic corporate information like client data and protected innovation are at expanded danger. One of the most concerning drawbacks is the potential loss of control over some or the greater part of the cloud environment that houses the information. Distributed computing is regularly isolated into three primary administration sorts: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and every effects information control and administration a little in an unexpected way. With IaaS, the client may have full control of the real server design conceding them more hazard administration control over the earth and information. In PaaS, the supplier deals with the equipment and hidden working framework which restricts venture hazard administration capacities on those segments. With SaaS, both the stage and the foundation are completely overseen by the cloud supplier which implies if the hidden working framework or administration isn't arranged legitimately the information in the higher layer application may be at danger [23]. If information isn't legitimately secured, misfortune and introduction can happen in the cloud whether its a private on-reason cloud or an open one. Due to element versatility, administration reflection, and area straightforwardness gimmicks of distributed computing models, a wide range of uses and information on the cloud stage have no settled foundation and security limits. In the occasion of security rupture, its hard to confine a specific physical asset that has a risk or has been traded off. As the openness of cloud and imparting virtualized assets by multi-occupant, client information may be gotten to by others.

4. ANALYSIS

Overall analysis was suggested in table 1.

Table 1: Comparison on the Latest Trends

S.no	Authors	Year	Work	Gap
1	Vijay et al.[23]	2012	Creators considered a structural engineering where diverse administrations are facilitated on the cloud framework by different cloud clients (tenants).This model amplifies the hub controller with the usefulness of the Certification Authority to ensure the conduct of the occupant virtual machines.	Since the Node Controller is mindful of the element changes to the occupant virtual machine, it can guarantee that the guaranteed properties are fulfilled by the inhabitant virtual machines.
4	Irina et al. [24]	2012	They recommend a portion of the key advantages and the significant downsides that come around with swapping out administrations and foundation to an open cloud. Taking into account these profits and downsides, K.O. (thump out) criteria will be recognized, which can be seen as the base premise for secure cloud Environment.	Suggested techniques can be fully implanted.
5	Mehdi et al. [25]	2013	Creators reason for existing is to focus on cloud information stockpiling security and to deal with the client's information in the cloud by Implementation of Kerberos validation Service.	Other standard encryption techniques can also be used.
6	Saravanakumar et al. [26]	2014	An inter-cloud and intra-cloud standard of cloud interoperability has been identified in order to highlight the challenges exist during the cloud interaction has been suggested.	Their report says that there is no standard will give a correct solution among various cloud and its services.
7	Fawaz S. Al-Anzi[27]	2014	They focus on the area, i.e. application security, information security, infrastructure security and security monitoring by giving our own security model.	Physical assets should be implemented.

8	Zhao et al. [28]	2014	Their new security solution is fully fit for the processing and retrieval of the encrypted data and effectively leading to the broad applicable prospect, the security of data transmission and the storage of the cloud computing.	Further analysis should be needed.
9	Dinadayalan et al. [29]	2014	The basic problem of cloud computing and describes the data security and privacy protection issues in cloud.	It should be tested on different platforms.

5. CONCLUSION AND FUTURE WORK

As per the study and analysis presented in this paper cloud computing platform has been in the greater demand due to scalability, interoperability, pay per use and virtualization etc. The security in cloud computing is the major concern as the use of cloud computing is increases day by day. So as per our analysis a hybrid framework is needed to secure the shared data. There are several way to protect the data in the cloud environment, as per our study different standard encryption techniques like DES, RSA, RC4, AES etc. can be applied for data aggregation and distribution. This can help to protect the password to protect in two ways through sender and receiver. The second approach can be detect on time the attack and prevent it on the fly through the use of secure virtualization.

6. REFERENCES

[1] 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.

[2] 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.

[3] Adigun A. Adebisi, Adegun A. Adekanmi, Asani E. Oluwatobi, " A Study of Cloud Computing in the University Enterprise " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.450-458.

[4] Abdur Rahim Choudhary, "Baseline Requirements and Architecture for Cloud Computing Services", International Journal of Advanced Computer Research (IJACR), Volume-2, Issue-7, December-2012, pp.1-7.

[5] 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.

[6] Gaurav, Nitesh Kaushik, Jitender Bhardwaj, " A Computation Offloading Framework to Optimize Makespan in Mobile Cloud Computing Environment " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.442-449.

[7] 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.

[8] 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.

[9] Adigun Abimbola Adebisi, Akande Noah Oluwatobi and Ajagbe Oluwafemi Adeola, " Design and Implementation of a Mobile Students' Course Registration Platform " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-3, February-2015 ,pp.25-30.

[10] 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.

[11] 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.

[12] 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.

[13] Sanjay Kumar Brahman, Brijesh Patel, "Data sharing and Management based on RC4 in User Cloud Environment", International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-12, September-2013 ,pp.201-206.

[14] 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.

[15] 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.

[16] 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.

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

[18] 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.

[19] Khalil, I.M.; Khreishah, A.; Bouktif, S.; Ahmad, A., "Security Concerns in Cloud Computing," Information Technology: New Generations (ITNG), 2013 Tenth International Conference on , vol., no., pp.411,416, 15-17 April 2013.

[20] M.Krishnaveni, P.Subashini, A.Vanitha, "A Bayes fusion method based ensemble classification approach for Brown cloud application" , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-14, March-2014 ,pp.299-304.

[21] Benameur, A.; Evans, N.S.; Elder, M.C., "Cloud resiliency and security via diversified replica execution and monitoring," Resilient Control Systems (ISRCS), 2013 6th International Symposium on, pp.150, 155, 13-15 Aug. 2013.

[22] Liu Xiao-hui; Song Xin-fang, "Analysis on cloud computing and its security," Computer Science & Education (ICCSE), 2013 8th International Conference on, vol., no., pp.839,842, 26-28 April 2013.

[23] Varadharajan, Vijay, and Udaya Tupakula. "TREASURE: Trust enhanced security for cloud environments." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pp. 145-152. IEEE, 2012.

[24] Astrova, Irina, Stella Gatziu Grivas, Marc Schaaf, Arne Koschel, Jan Bernhardt, Mark Dennis Kellermeier, Stefan Nitz, Francisco Carriedo Scher, and Michael Herr. "Security of a Public Cloud." In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, pp. 564-569. IEEE, 2012.

[25] Hojabri, M., and K. V. Rao. "Innovation in cloud computing: Implementation of Kerberos version5in cloud computing in order to enhance the security issues." In Information Communication and Embedded Systems (ICICES), 2013 International Conference on, pp. 452-456. IEEE, 2013.

[26] Saravanakumar, C.; Arun, C., "Survey on interoperability, security, trust, privacy standardization of cloud computing," Contemporary Computing and Informatics (IC3I), 2014 International Conference on , vol., no., pp.977,982, 27-29 Nov. 2014.

[27] Al-Anzi, F.S.; Yadav, S.K.; Soni, J., "Cloud computing: Security model comprising governance, risk management and compliance," Data Mining and Intelligent Computing (ICDMIC), 2014 International Conference on , vol., no., pp.1,6, 5-6 Sept. 2014

[28] Zhao, Feng, Chao Li, and Chun Feng Liu. "A cloud computing security solution based on fully homomorphic encryption." Advanced Communication Technology (ICACT), 2014 16th International Conference on. IEEE, 2014.

[29] Dinadayalan, P., S. Jegadeeswari, and D. Gnanambigai. "Data Security Issues in Cloud Environment and Solutions." Computing and Communication Technologies (WCCCT), 2014 World Congress on. IEEE, 2014.