International Journal of Advanced Technology and Engineering Exploration, Vol 3(15)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2016.315001

Review Article

A meta-analysis on secure cloud computing

Bhupendra Kumar[1*] and Jayshree Boaddh[2]
Student, Department of Computer Science, MIT, RGPV, Bhopal[1]
Assistant Professor, Department of Computer Science, MIT, RGPV, Bhopal[2]

Abstract
In today's era there is a vast demand of cloud computing because of the easy to maintain infrastructure with low cost. It is used in several areas including University, Hospital, E-Commerce and file storage services. This increasing demand of cloud computing is increasing day by day. As the peoples are growing in this platform also indicates the chances of malpractices and data theft. So this paper objective is to analyses the security threats which can be possible in cloud computing environment and suggest some effective steps to overcome. This paper also highlights the methodological reviews which are already done with their pros and cons.

Keywords
Cloud Computing, Security, Data Handling, methodological reviews.

1.Introduction
Cloud computing give on interest assets in light of pool of assets accessible by the cloud suppliers [1][2][3]. From the part of customary registering the benefits of distributed computing are: nimbleness, lower section cost, gadget independency, area independency, and adaptability [4][5]. Be that as it may, the security concerns are the real key viewpoints later on distributed computing time. 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. In any case, to accomplish the execution on the parallel framework and keeping up the respectability is extreme [11].

In every one of these works, incredible endeavours are made to plan arrangements that meet different prerequisites: high plan effectiveness, stateless check, unbounded utilization of questions and hopelessness of information, and so on. Considering the part of the verifier in the model, every one of the plans exhibited before fall into two classes: 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 component of distributed computing by which information sharing is conceivable between diverse machines of virtual presence from the server farm [12].

Virtualization empowers the live relocation [9] 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 shopper furthermore to balance load crosswise over physical servers in the information centers[12].

The main cloud providers are [13] Google, Microsoft, Amazon and Salesforce.com. The cloud computing service model relies on the data communication layer. The whole communication is relies on three layers. The first layer is Software as a Service (SaaS) which is mainly transformed on desktop based applications into online software products that can be used worldwide. A generally utilized application is Salesforce.com, a client relationship administration (CRM) programming for interfacing with organizations and clients [14]. As indicated by [14] 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) for the most part includes virtualization situations as acquired administrations as opposed to physical or committed PC hardware.

*Author for correspondence

In the conventional method for figuring the assets are acquired locally which are once in a while higher in expense and not reasonable. This limits the routes in which a client could cooperate with the product in that the product was just accessible and available for the first workstation [14]. However, now by the utilization of distributed computing the Software as a Service model has changed this philosophy in a manner that product can be bought for use over the Internet [14]. Rather than obtaining programming in a boxed configuration, the client can buy an administration to utilize an application that is facilitated in the cloud [14]. In [15] contrasting private cloud and open cloud , records contrasts in the middle of them and advances a building design of private distributed computing to bolster savvy brace, explains structure of every layer, and shows idea of private distributed computing working framework and system virtualization. In [16] displayed a contextual analysis utilizing online Personal Health Record (PHR), they first demonstrate the need of pursuit ability approval that lessens the security presentation coming about because of the list items, and set up a versatile structure for Authorized Private Keyword Search (APKS) over scrambled cloud information. In [17] authors proposed that Storage-as-an administration is a crucial part of the distributed computing framework. To connect this crevice, they propose a down to earth multi-client searchable encryption plan, which has various points of interest over the known methodologies. In [21] recommend Healthcare, training, business, and numerous different areas take a gander at distributed computing as a try to comprehend the ceaseless deficiency in volume, foundation, availability, and observing strength. In [18] proposed that distributed computing has been imagined as the cutting edge building design of IT Enterprise. In [25] recommended that the information security and protection on cloud is a critical issue, turning into the greatest hindrance of distributed computing advancement. In [26] proposed homomorphism encryption algorithm in the cloud computing to solve the problem of data security. The principle advantage of this sort of framework arrives 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 incorporated with the security administrations it turns out to be intense.

2.Literature survey

The previous methodology literature and analysis is shown in *table1*.

Table 1 Literature review

S.No	Authors	Work	Gap
1	Gupta et al. [27]	They investigates the cloud security dangers furthermore talks about the current security ways to deal with secure the cloud environment .They additionally proposed a novel Tri-system for cloud security against information break which give all around security to the cloud structural planning.	They have not suggested the situation when there is the possibility of attack.
2	Syed Naqvi et al. [19]	They have presented a formal method for testing the effect of adaptability and heterogeneity on the united Cloud security administrations.	They have suggested the need of more complex policy rules to better reflect the emerging security requirements.
3	Huaglory Tianfield et al. [20]	Presented an exhaustive study on the difficulties and issues of security in distributed computing. They first investigate the effects of the unmistakable attributes of distributed computing, to be specific, multi-tenure, versatility and outsider control, upon the security prerequisites.	The practical implications of the issues are missing.
4	Dubey et al. [5]	They proposed a new cloud computing environment where we approach a trusted cloud environment which is controlled by both the client and the cloud environment admin. Their approach is mainly divided into two parts. First part is controlled by the normal user which gets permission by the cloud environment for performing operation	The practical implications are missing.

		and for loading data. Second part shows a secure trusted computing for the cloud, if the admin of the cloud want to read and update the data then it take permission from the client environment. This provides a way to hide the data and normal user and can protect their data from the cloud provider. This provides a two way security protocol which helps both the cloud and the normal user.	
5	Wentao Liu et al. [22]	They have proposed that the security issue of distributed computing is vital and it can keep the fast improvement of distributed computing.	How to prevent the data misuse is not discussed properly.
6	Nikhilesh Pant et al. [23]	They have presented the procedures for cloud appropriation and cloud security appraisal to investigate potential security and consistence suggestions in cloud environment.	They have not suggested the situation when there is the possibility of attack.
7	Du meng et al. [24]	They have suggested distributed computing information security issues, including tile security of information transmission, stockpiling, security and administration of security.	The methods are need to be explained in detail.
8	Mehdi et al. [30]	Authors purpose is to concentrate on cloud data storage security and to manage the user's data in the cloud by Implementation of Kerberos authentication Service.	Other standard encryption techniques can also be used.
9	Liu Xiao-hui et al. [31]	Authors introduced cloud development status, and analysed the security problems.	The security problem has become a focus
10	Azzedine Benameur et al. [32]	Authors present an approach to leverage the elasticity and on-demand provisioning features of the cloud to improve resilience to availability concerns and common attacks.	Need of supporting different file formats.
11	Yang CN et al. [33]	Authors provide comprehensive study of cloud computing security that includes classification of known security threats and the state-of-the-art practices in the endeavor to calibrate these threats. They also provides the dependency level within classification and provides a solution in form of preventive actions rather than proactive actions.	Cloud computing security such as auditing, side channels and migration of data from one cloud to another. Emphasis has always been on fast performance and low cost but the quality of service has not been considered.
12	Qian Wang et al. [34]	Authors deal with cloud security services including key agreement and authentication. By using Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing, authors design the secure cloud computing (SCC).	It can be extended to multi-layer security scheme.
13	Dubey et al. [35]	This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud.	Other standard encryption techniques can also be used to enhance the security.

3.Problem domain

Based on the above discussion we have found following gaps:

1. There are couple of territories which are still unattended in distributed computing security, for example, inspecting, side channels and movement of information starting with one cloud then onto the next [28].
2. Privacy preserving algorithms can be applied to cloud computing security [29].
3. Standard encryption algorithm can be applied for securing cloud data [5].
4. Enterprises ought to dependably expect to deal with the encryption keys, yet in the event that they are overseen by a cloud encryption supplier; Gartner says they must guarantee access administration controls are set up that will fulfil break notice necessities and information residency.
5. If keys are overseen by the service provider then organizations ought to require equipment based key administration frameworks inside of a firmly characterized and oversaw set of key administration forms.
6. Not All information requires approach insurance, so organizations ought to classes information planned for distributed storage and recognize any consistence necessities in connection to information rupture notice or if information may not be put away in different purviews.
7. Security should be maintained by the providers as well as the client and it should be controlled equally.

4.Proposed algorithm

For providing better security a hybrid encryption algorithm based on AES and RSA is presented.

Algorithm 1: AES based RSA Algorithm

In this algorithm we have used 128-bit key. It is ordered in the similar matrix by column.

Step 1: Plain text as an input.

Step 2: The key that is given as data is ventured into a cluster of 44 words (32-bits each), w[i]. 4 distinct words (128 bits) serve as a round key for each round.

Step 3: 4 distinct stages are utilized, 1 change and 3 of substitution:

- Substitute bytes–Uses a S-box to perform a byte-to-byte substitution of the piece

-Shift lines–A basic change

-Mix sections–A substitution that makes utilization of number juggling.

-Add round key–A straightforward bitwise XOR of the present square with the bit of the extent.

Step 4: It shows the encryption round uses arithmetic in the finite field that is Galois field GF (2^7), with the irreducible polynomial.

Step 5: Just the Add Round Key stage utilizes the key. Whatever other stage is reversible without learning of the key.

Step 6: The Add Round Key is a type of Vernam cipher and independent from anyone else would not be imposing.

The other 3 organizes together give disarray, dispersion, and nonlinearity, however without anyone else would give no security in light of the fact that they don't utilize the key. Then the data is adjusting according to the XOR encryption with the added round key. The stage is also completely reversible

Step 7: Then encryption process is applied with the same keys.

The encryption key (e,n), is calculated in the following way:

Step 1: The public/private key pair is generated by the following steps:

Choose two large primes at random – a,b

Step 2: Caculate system modulus N=a.b

ø(N)=(a-1)(b-1)

Step 3: Encryption key e is now choosen in this manner that the e lies in $1<e<ø(N)$, $gcd(e,ø(N))=1$

Step 4: Decryption key d is calculated then

$e.d=1 \bmod ø(N)$ and $0 \le d \le N$

Step 5: public encryption key: KU={e,N}

Step 6: private decryption key: KR={d,a,b}

Step 7: For encrypting the message M first receive the public key of the receiver: KU={e,N}

$C=M^e \bmod N$, where $0 \le M < N$

Step 8: For deecrypting it use the private key KR={d,a,b} $M=C^d \bmod N$

5.Conclusion and future work

This paper provides the background for data security in cloud computing environment. According to this review and analysis the data security will be needed in three directions first through the client, through the cloud and third is on the data by using some standard encryption techniques.

Based on the observations we can suggest that the secure model can be developed by using standard encryption techniques or by using hybridization of these techniques. Classification and categorization [36] can be used for data pre-processing. Proper virtualization can be protected with the affinity aware colocation [37].

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, et al. Above the clouds: A Berkeley view of cloud computing. Department Electrical Engineering and Computer Sciences, University of California, Berkeley, Rep. UCB/EECS. 2009; 28(13).
[2] Ruiz-Agundez I, Penya YK, Bringas PG. Cloud computing services accounting. International Journal of Advanced Computer Research (IJACR). 2012; 2(2); 7-17.
[3] Singh A, Shrivastava M. Overview of security issues in cloud computing. International Journal of Advanced Computer Research (IJACR); 2012; 2(3); 41-5.
[4] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, et al. Provable data possession at untrusted stores. In proceedings of the 14th ACM conference on computer and communications security 2007 (pp. 598-609). ACM.
[5] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering (CONSEG) 2012 (pp.1-8). IEEE.
[6] Juels A, Kaliski Jr BS. PORs: Proofs of retrievability for large files. In proceedings of the 14th ACM conference on computer and communications security 2007 (pp. 584-97). ACM.
[7] Shacham H, Waters B. Compact proofs of retrievability. Journal of Cryptology. 2013; 26(3):442-83.
[8] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. In proceedings of the 2009 ACM workshop on Cloud computing security 2009 (pp. 43-54). ACM.
[9] Naor M, Rothblum GN. The complexity of online memory checking. In foundations of computer science. 46th annual IEEE symposium 2005 (pp. 573-82). IEEE.
[10] Tsai WT, Sun X, Balasooriya J. Service-oriented cloud computing architecture. In seventh international conference on information technology: new generations (ITNG), 2010 (pp. 684-89). IEEE.
[11] Patra GK, Chakraborty N. Securing cloud infrastructure for high performance scientific computations using cryptographic techniques. International Journal of Advanced Computer Research. 2014; 4(1):66-72.
[12] Pachorkar N, Ingle R. Multi-dimensional affinity aware VM placement algorithm in cloud computing. International Journal of Advanced Computer Research. 2013; 3(4):121-5.
[13] http://www.dialogic.com/~/media/products/docs/white papers/12023-cloud-computing-wp.pdf. Accessed 26 October 2015.
[14] Tschinkel B. Cloud computing security understanding risk areas & management techniques. 2011.
[15] Zheng L, Hu Y, Yang C. Design and research on private cloud computing architecture to support smart grid. In international conference on intelligent human-machine systems and cybernetics (IHMSC) 2011(pp. 159-61). IEEE.
[16] Li M, Yu S, Cao N, Lou W. Authorized private keyword search over encrypted data in cloud computing. In international conference on distributed computing systems (ICDCS) 2011 (pp. 383-92). IEEE.
[17] Yang Y. Towards multi-user private keyword search for cloud computing. In international conference on cloud computing (CLOUD) 2011 (pp. 758-9). IEEE.
[18] Wang Q, Wang C, Ren K, Lou W, Li J. Enabling public auditability and data dynamics for storage security in cloud computing. , IEEE Transactions on Parallel and Distributed Systems. 2011; 22(5):847-59.
[19] Naqvi S, Michot A, Van de Borne M. Analysing impact of scalability and heterogeneity on the performance of federated cloud security. In 11th international conference on trust, security and privacy in computing and communications (TrustCom) 2012 (pp. 1137-42). IEEE.
[20] Tianfield H. Security issues in cloud computing. In international conference on systems, man, and cybernetics (SMC) 2012 (pp. 1082-9). IEEE.
[21] Abuhussein A, Bedi H, Shiva S. Evaluating security and privacy in cloud computing services: A stakeholder's perspective. In international conference for internet technology and secured transactions 2012 (pp. 388-95). IEEE.
[22] Liu W. Research on cloud computing security problem and strategy. In 2nd international conference on consumer electronics, communications and networks (CECNet) 2012 (pp. 1216-19). IEEE.
[23] Pant N, Parappa S. Seeding the cloud in a secured way: cloud adoption and security compliance assessment methodologies. In 4th international conference on software engineering and service science (ICSESS) 2013 (pp. 305-8). IEEE.
[24] Du Meng, Data security in cloud computing. In 8th international conference on computer science & education (ICCSE) 2013 (pp. 810-3). IEEE.
[25] Yang F, Pan L, Xiong M, Tang S. Establishment of security levels in trusted cloud computing platforms. In green computing and communications (GreenCom), 2013 IEEE and internet of things (iThings/CPSCom), IEEE international conference on and IEEE cyber, physical and social computing 2013 (pp. 2119-22). IEEE.
[26] Zhao F, Li C, Liu CF. A cloud computing security solution based on fully homomorphic encryption. In international conference on advanced communication technology (ICACT) 2014 (pp. 485-8). IEEE.
[27] Gupta A, Chourey V. Cloud computing: security threats & control strategy using tri-mechanism. In international conference on control, instrumentation, communication and computational technologies (ICCICCT) 2014 (pp. 309-16). IEEE.

[28] Khalil IM, Khreishah A, Bouktif S, Ahmad A. Security concerns in cloud computing. In tenth international conference on information technology: New Generations (ITNG) 2013 (pp. 411-6). IEEE.
[29] Agarwal V, Khandagre Y, Dubey AK. Novel cloud subset preserving mining (CSPM) algorithm for association rule mining in centralized database. In international conference on technology enhanced education (ICTEE) 2012 (pp. 1-5). IEEE.
[30] Hojabri M, Rao KV. Innovation in cloud computing: implementation of Kerberos version 5 in cloud computing in order to enhance the security issues. In international conference on information communication and embedded systems (ICICES), 2013 (pp. 452-6). IEEE.
[31] Xiao-hui L, Xin-fang S. Analysis on cloud computing and its security. In international conference on computer science & education (ICCSE) 2013 (pp. 839-42). IEEE.
[32] Benameur A, Evans NS, Elder MC. Cloud resiliency and security via diversified replica execution and monitoring. In 6th international symposium resilient control systems (ISRCS), 2013 (pp. 150-5). IEEE.
[33] Yang CN, Lai JB. Protecting data privacy and security for cloud computing based on secret sharing. In international symposium on biometrics and security technologies (ISBAST) 2013 (pp. 259-66). IEEE.
[34] Wang Q, Wang C, Ren K, Lou W, Li J. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(5):847-59.
[35] Dubey AK, Dubey AK, Agarwal V, Khandagre Y. Knowledge discovery with a subset-superset approach for mining heterogeneous data with dynamic support. In CSI Sixth international conference on software engineering (CONSEG) 2012 (pp. 1-6). IEEE.
[36] Dubey AK, Kushwaha GR, Shrivastava N. Heterogeneous data mining environment based on DAM for mobile computing environments. In information technology and mobile communication 2011; 144-9. Springer Berlin Heidelberg.
[37] Pachorkar N, Ingle R. Affinity aware VM colocation mechanism for cloud. International Journal of Advanced Computer Research. 2014; 4(4):956-60.