International Journal of Advanced Technology and Engineering Exploration, Vol 3(17)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2016.317005

Research Article

A hybrid security approach based on AES and RSA for cloud data

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

Abstract
In this paper we have proposed an efficient and secure cloud computing framework which support security for the cloud users and data control is being provided at the cloud user side. The cloud user can use the privilege of inter cloud communication with the data security of AES and RSA security hybridization which will provide four key security. The encryption is provided by the server. Then the receiver cloud can view the request file by applying the four keys. If any malicious behaviour is identified before the cloud user read operation then our document identification bit alert the client and server for the possible attack. So this framework supports secure data inter communication with malicious identification also.

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 centres[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. In the conventional method for figuring the assets are acquired locally which are once in a while higher in expense and not reasonable.

*Author for correspondence

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]. 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

In 2011, Ling Zheng et al. [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. It gives the hypothetical reference to assemble the private distributed computing, in this way advances the development of the keen network.

In 2011, Ming Li et al. [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. They then propose two novel answers for APKS in light of a late cryptographic primitive, Hierarchical Predicate Encryption (HPE). Their answers empower proficient multi-dimensional catchphrase seeks with reach inquiry; permit designation and renouncement of pursuit abilities. They upgrade the inquiry protection which shrouds clients' question catchphrases against the server.

In 2011, Yanjiang Yang et al. [17] propose that Storage-as-an administration is a crucial part of the distributed computing framework. Database outsourcing is a run of the mill use situation of the distributed storage administrations, wherein information encryption is a decent approach empowering the information proprietor to hold its control over the outsourced information. Searchable encryption is a cryptographic primitive taking into consideration private watchword based pursuit over the scrambled database. The setting of big business outsourcing database to the cloud requires multi-client searchable encryption, while for all intents and purposes every single existing plan consider the single-client setting. 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 2011, Wang et al. [18] proposed that distributed computing has been imagined as the cutting edge building design of IT Enterprise. It moves the application programming and databases to the concentrated extensive server farms, where the administration of the information and administrations may not be completely dependable. A creator concentrates on the issue of guaranteeing the respectability of information stockpiling in Cloud Computing. Specifically, they consider the assignment of permitting an outsider inspector (TPA), for the benefit of the cloud customer, to check the trustworthiness of the dynamic information put away in the cloud. The presentation of TPA kills the association of the customer through the evaluating of whether his information put away in the cloud is for sure in place, which can be essential in accomplishing economies of scale for Cloud Computing.

In 2012, Syed Naqvi et al. [19] present a formal method for testing the effect of adaptability and heterogeneity on the united Cloud security administrations. Their expects to build up a mean of measuring the effect on security capacities under different working conditions and parameters of unified Cloud arrangements. Their aftereffects of this work will assist organizations with identifying the best security structural planning that will fit their Cloud architectures and execution prerequisites.

In 2012, Huaglory Tianfield et al. [20] present 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. At that point, they dissect the cloud security necessities regarding the principal issues, i.e., privacy, respectability, accessibility, trust, and review and consistence. They talk about the scientific categorization for security issues in distributed computing. They outline the security issues in distributed computing by cloud security building design.

In 2012, Abdullah Abuhussein et al. [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. On the other hand, moving information to the cloud suggests moving control of the client's information to the cloud administration supplier inconclusively. Thus, the security and protection of the client's data turns into an essential issue. Surveying 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 adequate and hearty in the meantime. They endeavors to recognize and classify a rundown of characteristics which mirror the different parts of cloud security and protection. These credits can be utilized to survey and analyze distributed computing administrations with the goal that customers 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. [22] 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 breaks down distributed computing security issue and its procedure as indicated by 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 conventional and new advances and methodologies must be utilized together to protect the aggregate distributed computing framework.

In 2013, Nikhilesh Pant et al. [23] present the procedures for cloud appropriation and cloud security appraisal to investigate potential security and consistence suggestions in cloud environment. They talks about in subtle element on how an association may continue for security and consistence appraisal amid the cloud calculation. Their methodology and ideas point by point in this paper would be valuable for associations that are included in the cloud reception process.

In 2014, Liu X. [24] talks about distributed computing information security issues, including tile security of information transmission, stockpiling, security and administration of security. Concentrate on all inclusive information administration influence cloud security examination, and pointed out that a leap forward in the advancement of this distributed computing, attempt to list the comparing methodologies and long haul improvement heading.

In 2013, Fan Yang et al. [25] recommended that the information security and protection on cloud is a critical issue, turning into the greatest hindrance of distributed computing advancement. A Trusted Cloud Computing Platform (TCCP) in view of remote validation constructs a trusted cloud for inhabitant. The basic segment is incorporated Trusted Coordinator, taking the spot of occupants to verify hubs separately in distributed computing stage. In any case, when a great deal of inhabitants apply for hubs in the meantime, Trusted Coordinator (TC) possibly 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, each in charge of confirming diverse application kind. The distinctive validation arrangements, for example, client secret word examination, picture hash check and trusted chain estimation, as indicated by diverse security levels. In 2014, Zhao et al. [26] proposed homomorphism encryption algorithm in the cloud computing to solve the problem of data security. According to the authors this can fit for processing and retrieval of the encrypted data and it is effectively applicable for data transmission and the storage. In 2015, Gupta et al. [27] has been envisioned as a cutting edge structural planning of IT Industries. Security and protection is the significant obstacle in the cloud environment as a result of its transparent construction modeling. 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.

3.Proposed algorithm

Our proposed approach provides security with two standard encryption mechanisms namely Advanced Encryption Standard (AES) and Ron Rivest, Adi Shamir, and Leonard Adlema (RSA) mechanism. In this approach the enlisted client first chooses the server from the 4 determined previously. Space is overseen for all intents and purposes and it will migrate the space according to the interest by the client with no interference. The information is then transferred in the chose server as asked for by the

client and it is then accessible for the self-use reason promptly. The information is then accessible to share to other authorized clients in the cloud from any four servers. For the testing case we have confined the document sort to message just so that legitimate correlation can be given the same kind of information. On the off chance that the enrolled client needs to get to the information of other client, it can be gotten to on solicitation to the specific client through the cloud administration. If the user which is registered in this solicited environment wants to access the data of any other registered user, it can only be permitted through this environment based on the request grant of that particular user not the client. This is the first enhancement of our work. Implies our work gives information offering capacity yet to the safe information exchange. The client information is confined for perspective to the cloud suppliers so information read consent is not for cloud suppliers too. This is the second strength of this work. In the event that the other cloud client consents to share the information to another cloud client then the information is readied for sending it to the regarded cloud client. The information is transferred with AES and RSA mechanism system and the plaintext is changed to content as indicated by AES and RSA both. It provides four key security. This is the next advancement of our work. At that point an information bit document is send with the information that will consequently render the notice to the administration supplier if the not assigned client will open the record first. As the security is by standard encryption strategy it will give a superior and solid against denial of service. This is the third idea included our system. At that point the beneficiary can get to the information subsequent to applying both AES and RSA encryption standard component. In the event that some other client opens the records the information bit alarms the bungle operation to the cloud supplier. The keys are irregular created so for the same record the keys are distinctive. So following it is distinctive.

We have likewise kept up the effective virtualization system which will empower the vitalization space as indicated by the prerequisite. So that the heap will be appropriately conveyed. This is the fourth point of interest of our work. In this we have received 500 KB + record size plan for this instrument. Implies the space will consequently procure the space 500 Kb + size of the records which is to be transferred.

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} $M=C^d \bmod N$

4.Results and evaluation

Different tables are used to maintain efficiently the data in the cloud environment at the server side in our approach. Our alerts times shows this mechanism with time calculation (in milliseconds) when server knows the information about the change of data. Our cloud server alerts times shows that our mechanism is far better than previous mechanism.

The results from our methodology are discussed and shown below. *Table 1* shows the log of all the data uploaded in any of the server on the cloud environment. *Table 2* shows the size changes in the process of encryption and decryption. It also shows the time in the process for encryption and decryption. *Table 3* shows the time for the malicious behaviour identification in the process of cryptography. *Figure 1* shows the time analysis in the mean process of encryption. *Table 4* shows the automated process of virtualization in all the server modes. *Figure 2* shows the malicious behaviour analysis based on different users

Table 1 Log of data uploaded

File Name	User Name	Server Name	Upload Date	Open	Public
do2.doc	RAJESH	server2	Tue Mar 08 07:21:20 IST 2016	yes	0000
word1.doc	rajesh	server2	Tue Mar 15 15:28:26 IST 2016	yes	0000
Text4.txt	rajesh	server2	Tue Mar 15 15:28:46 IST 2016	yes	0000
Web3.html	rajesh	server2	Tue Mar 15 15:28:59 IST 2016	yes	0000
Text4.txt	sumit	server3	Tue Mar 15 15:32:29 IST 2016	yes	0000
do2.doc	sumit	server4	Tue Mar 08 07:32:52 IST 2016	yes	65537
do2.doc	sumit	server4	Tue Mar 15 15:36:02 IST 2016	yes	65537
do2.doc	amit	server4	Tue Mar 15 15:37:21 IST 2016	no	65537
do2.doc	sumit	server4	Tue Mar 08 22:01:25 IST 2016	yes	65537
do2.doc	sumit	server4	Tue Mar 08 07:37:28 IST 2016	yes	65537
word1.doc	sumit	server4	Tue Mar 15 15:36:17 IST 2016	no	65537
Text4.txt	sumit	server4	Tue Mar 15 15:35:47 IST 2016	yes	65537
Text4.txt	amit	server4	Tue Mar 15 15:36:52 IST 2016	no	65537
Web3.html	sumit	server4	Tue Mar 15 15:36:10 IST 2016	no	65537
popop.txt	paramj	server4	Fri Mar 04 04:54:12 IST 2016	yes	65537
lion.txt	paramj	server4	Sat Mar 05 21:24:19 IST 2016	yes	65537

Table 2 Size and time in encryption and decryption process

Status	E-Size(Kb)	D-Size(Kb)	E-T(Ms)	D-T(Ms)
safe	24576	0	0	0
safe	761	0	0	0
safe	2913	0	0	0
safe	471	0	0	0
safe	2913	0	0	0
safe	24576	49536	5741	2242
safe	24576	49536	4750	4764
attack	24576	49536	2665	2786
safe	24576	49536	6942	3245
safe	24576	49536	10468	9876
attack	761	1548	1467	803
safe	2913	5934	4230	4170
attack	2913	3824	3556	2567
attack	471	1032	1446	1026
safe	658	1548	6022	1146
safe	397	1032	5195	3416

Table 3 Malicious behaviour detection

User Name	File Name	Attack Time	Alert Time	Difference
amit	Text4.txt	Tue Mar 15 15:48:53 IST 2016	Tue Mar 15 15:48:54 IST 2016	640
amit	Text4.txt	Tue Mar 15 15:49:56 IST 2016	Tue Mar 15 15:49:56 IST 2016	22
sumit	Web3.html	Tue Mar 15 15:50:05 IST 2016	Tue Mar 15 15:50:05 IST 2016	35
sumit	word1.doc	Tue Mar 15 15:50:18 IST 2016	Tue Mar 15 15:50:18 IST 2016	23
amit	do2.doc	Tue Mar 15 15:50:28 IST 2016	Tue Mar 15 15:50:28 IST 2016	27

Table 4 Server size virtualization

Server Name	Total Space	Used Space	Free Space
server1	90000	4194	85806
server2	40000	32109	7891
server3	160000	24260	135740
server4	140000	107586	-107586

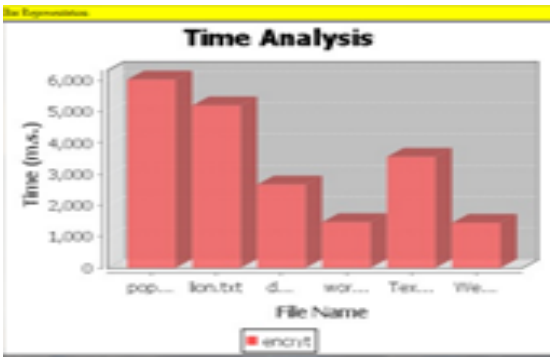

Figure 1 Encrypted file size time anaysis

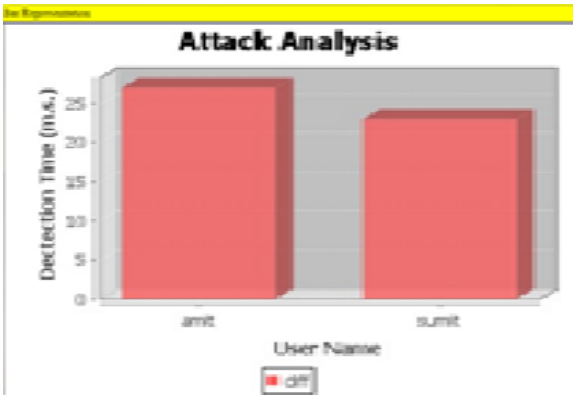

Figure 2 Attack analysis

5.Conclusion

In this paper we have designed a secure user cloud framework with the help of AES and RSA algorithms. Our approach provides an authenticated way of entering the cloud user and provides inter clod communication virtualization environment. For data security in inter cloud communication AES and RSA capability are used as the four key security. The key control with the user side protection is the main benefit of our dissertation. Then we have provided the data identification bit control for controlling any malicious behaviour detection.

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 engineer and computer sciences, University of California, Berkeley, Rep. UCB/EECS. 2009; 28(13); 1-42.

[2] Ruiz-Agundez I, Penya YK, Bringas PG. Cloud computing services accounting. International Journal of Advanced Computer Research. 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, Song D. 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 46th annual IEEE symposium on foundations of computer science 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. 684-9). IEEE.

[11] Patra GK, Chakraborty N. Securing cloud infrastructure for high performance scientific computations using cryptographic techniques. International Journal of Advanced Computer Research (IJACR). 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 10 January 2016.

[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 31st 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 IEEE 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. Analyzing impact of scalability and heterogeneity on the performance of federated cloud security. In IEEE 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 IEEE 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 international conference on consumer electronics, communications and networks (CECNet) 2012 (pp. 1216-9). IEEE.

[23] Pant N, Parappa S. Seeding the cloud in a secured way: cloud adoption and security compliance assessment methodologies. In IEEE international conference on software engineering and service science (ICSESS) 2013 (pp. 305-8). IEEE.

[24] Liu X. Data security in cloud computing. In proceedings of the 2012 international conference on cybernetics and informatics 2014 (pp. 801-6). Springer New York.

[25] Yang F, Pan L, Xiong M, Tang S. Establishment of security levels in trusted cloud computing platforms. In green computing and communications (GreenCom), 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 16th 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.