Security Enhancement Framework For Cloud Computing Environment

Ambalgi Bheemashankar, Dr. A.C. Subhajini

Abstract: Cloud Computing is a practical, adaptable and demonstrated conveyance stage for giving business or consumer IT services over the Internet. In any case, cloud computing presents an additional degree of hazard since essential services are frequently re-appropriated to a third party, which makes it harder to keep up information security and protection, bolster information and administration accessibility, and show consistency. Cloud computing uses many innovations (Web 2.0, virtualization, SOA); In addition, the security issues we are examining here are identified the major vulnerabilities of these framework types and the major threats identified with cloud computing, as well as the condition for differentiation and detection Dangers with possible solutions.

Keywords: Cloud computing, Encryption, Security, Virtual Machine

1. INTRODUCTION

Cloud computing has been imagined as the cutting edge worldview in calculation. In the cloud computing condition, the two applications and assets are conveyed on-request over the Internet as services. Cloud is an environment of the hardware and programming assets in the server farms that give different services over the system or the Internet to fulfill client's prerequisites. Cloud computing can be considered as another computing prime example that can give services on request at a negligible expense [1]. The three surely understood and ordinarily utilized help models in the cloud paradigm SaaS, PaaS and IaaS. In SaaS, programming with the related information is sent by a cloud specialist organization, and clients can utilize it through the internet browsers. In PaaS, a specialist organization encourages services to clients with a lot of programming programs that can unravel the particular undertakings. In IaaS, the cloud professional organization encourages services to clients with virtual machines and capacity to improve their business abilities [2]. Cloud computing includes the arrangement and utilization of IT infrastructure, platforms and uses of any sort as services that are electronically accessible on the Internet [3]. Only a couple of instances of uses utilizing cloud services include: online record stockpiling, long range interpersonal communication destinations, email, and online industry applications [4]. As undertakings endeavor to recognize new strategies for driving their organizations forward, flooding request has moved to arrangements that give lower-cost answers for utilization of computing frameworks (both regarding access to computing infrastructure and working expenses). This brought about the exponential growth of CC, which was observed to be more compelling than the prior arrangements [5]. As mechanical advances proceed, the span and impact of cloud computing keep on rising. All things being equal, when associations redistribute information and business applications to CC suppliers (who are outsiders for them), security and protection issues develop as pivotal concerns.

- *Ambalgi Bheemashankar, Research Scholar, Dept. of Computer Science, Sri SatyaSai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.*
- *Dr. A.C. Subhajini, Research Guide, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India.*

Virtualization is one of the key innovations of cloud computing services, offices, collection of numerous independent frameworks into single equipment platform by virtualizing computing resources (e.g.: Network, CPU's, Memory, Storage). Virtualization is empowered by equipment reflection, which conceals the multifaceted nature of dealing with the physical computing platform and streamlines adaptability of computing resources. It is executed through hypervisors [6]. A hypervisor is in charge of segregation of VMs, with the goal that they are kept from to legitimately getting to other VMs' virtual circles, memory, or applications on a similar host. Virtualization gives adaptability and multi-occupancy (the last happens when a solitary occasion of a software application serves different clients [7]). These two properties are huge attributes of CC, and encourage sharing and pooling of resources so as to improve deftness, adaptability, decrease expenses and upgrade business esteem. Security in the cloud is accomplished, partially, through third party controls and confirmation much like in conventional redistributing outsourcing arrangements. In any case, subsequently there is no basic cloud computing security standard, there are extra difficulties related with this. Many cloud sellers execute their own exclusive benchmarks and security advances and actualize diverse security models, which should be assessed alone merits. In a seller cloud model, it is at last down to embracing client associations to guarantee that security in the cloud meets their very own security approaches through necessities gathering provider hazard evaluations, due perseverance, and affirmation exercises.

Privacy and Security Issues In Cloud Computing

There are numerous safety issues for cloud computing as it incorporates various innovations including systems, databases, working frameworks, virtualization, asset booking, exchange the board, load balancing, simultaneousness control, and memory the executives. In this way, safety issues for a large number of these frameworks and innovations are material to cloud computing. For instance, the system that interconnects the frameworks in a cloud must be secure. Besides, the virtualization worldview in cloud computing prompts a few security concerns. For instance, representing the VM to the physical machines must be done safely. Information security includes encrypting the information just as guaranteeing that suitable arrangements are authorized for information sharing. Furthermore, asset designation and memory the board

calculations must be secure. As appeared in Figure 1, there are six explicit regions of the cloud computing condition where gear and programming require significant security consideration.

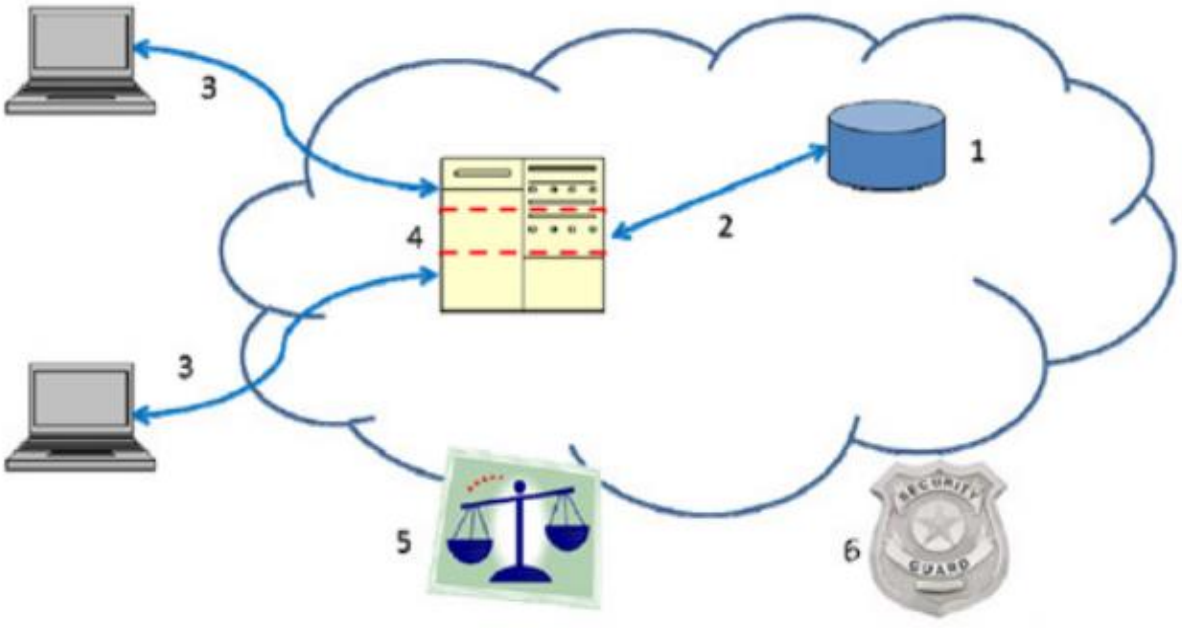

Figure 1. *Cloud computing security concerns*

These six zones are: (1) security of information, (2) security of information transit, (3) validation of clients/applications/forms, (4) robust separation between data belonging to different customers, (5) cloud legitimate and administrative issues, and (6) occurrence reaction. Cryptographic encryption systems are surely the best alternatives. The hard drive producers are currently delivering self-encrypting drives that execute confided away gauges of the confided in computing gathering. These self-encrypting drives incorporate encryption equipment with the drive, furnishing mechanized encryption with negligible expense or execution sway. That the product encryption can likewise be utilized for ensuring information, it causes the procedure to increasingly slow confirm since a foe might be able to receipts the “encryption key” from the machine without being recognized. The security challenges looked by associations wishing to utilize cloud services are not drastically unique in relation to those reliant on their own in-house oversaw undertakings. The equivalent inward and outer dangers are available and require chance relief or hazard acknowledgment. In the accompanying, we analyze the data security challenges that embracing associations should consider, either through confirmation exercises on the seller or open cloud providers or legitimately, through planning and actualizing security control in an exclusive cloud.

METHODOLOGY

The proposed strategy is likewise an uneven key cryptosystem which uses two keys for encryption and decoding. Public key consumed for encryption and comparing private key is applied for unscrambling. [9] Proposed 'n'prime number RSA cryptosystem. [10] Proposed another adaptation of RSA. Our proposed plan has drawn thought from these plans. In RSA, just two enormous prime numbers are considered while in our proposed encryption framework, we have taken four huge prime numbers. As in topsy-turvy key cryptography, the guide lies in how toward make it difficult for the aggressor to factorize n which is the augmentation of those four prime numbers. Our proposed framework isn't just about expanding prime numbers yet in addition we have connected security as far as public key and private key. In RSA, the public key comprises of e and n yet we have incorporated another parameter f. What's more, in private key, we have included three different parameters a, b and h.

Key Generation

1. Select four large prime numbers p, q, r and s such that they are all unique and not equal to each other.
2. n p x q x r x s
3. (n) (p-1) x (q-1) x (r-1) x (s-1)
4. Select e such that 1 < e < _(n) and e is coprime to _(n).
5. d e-1 mod _(n)
6. Select an integer b < _(n)-1
7. Pick another integer a such that b < a < _(n)
8. Pick another integer h such that a < h < _(n)
9. Calculate f=(ba)h
10. Public key (e, n, f)
11. Private Key (d, a, b, h)

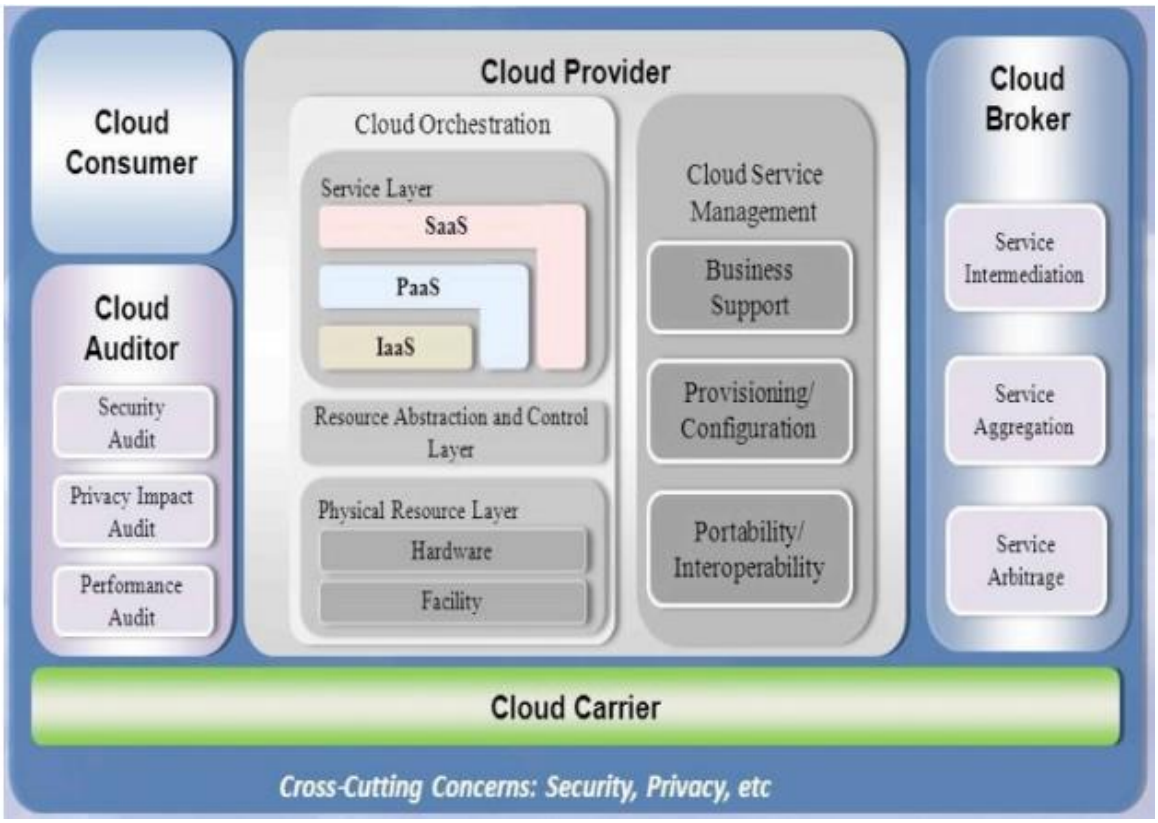

Figure 2. *Cloud Computing Security Architecture Approach (Source: NIST)*

Encryption

1. Let's say one party X wants to send a message to Y securely over an insecure channel.
2. Let's take 'e'be Y's public key. 'e'is known to A because 'e'is public key.
3. Now we want to apply our encryption scheme to the message or plain text P.
4. First, we have to convert the plaintext or message to an integer in the range 0 < P < n.
5. Now in the _nal step calculate cipher text which is C=(P x f)e mod n

Decryption

1. Let us consider C to be the cipher text which is received by Y from X.
2. Now we have to calculate the plain text from the received cipher text which can be derived as:- P= ((b_(n)-(a x h) mod n) x C)d mod n

So, in this way we can encrypt and decrypt data as per our requirements. The data can be encrypted using the public key and can be decrypted by the consistent private key as stated earlier.

RESULT AND DISCUSSION

Give us a chance to state we need to scramble a message as per our proposed awry key cryptosystem. Let's state the message is I am an understudy of sri satya Sai University, sehore. According to our proposed strategy, we initially need to choose four huge prime numbers which are one of a kind and not approach to anyone. In the wake of discovering those four prime numbers we must to figure the carrying work. The subsequent stage is to pick an arbitrary regular number e and after that ascertain the opposite of that number with modulus n where n is the result of those one of a kind prime numbers. Presently, we need to pick two other characteristic numbers which are not bigger than the carrying work.

Figure 3 demonstrates the substance of the record is encoded and is put away in bytes group as opposed to in plain content. On the off chance that an assailant gains admittance to the group and finds the information, it would not make much distinction as the information will be in unusable structure that is in encoded structure.

So as to decode it, he should factorize that enormous numbers into four novel prime numbers which is about inconceivable. Thusly we can beat the security dangers related with hadoop.

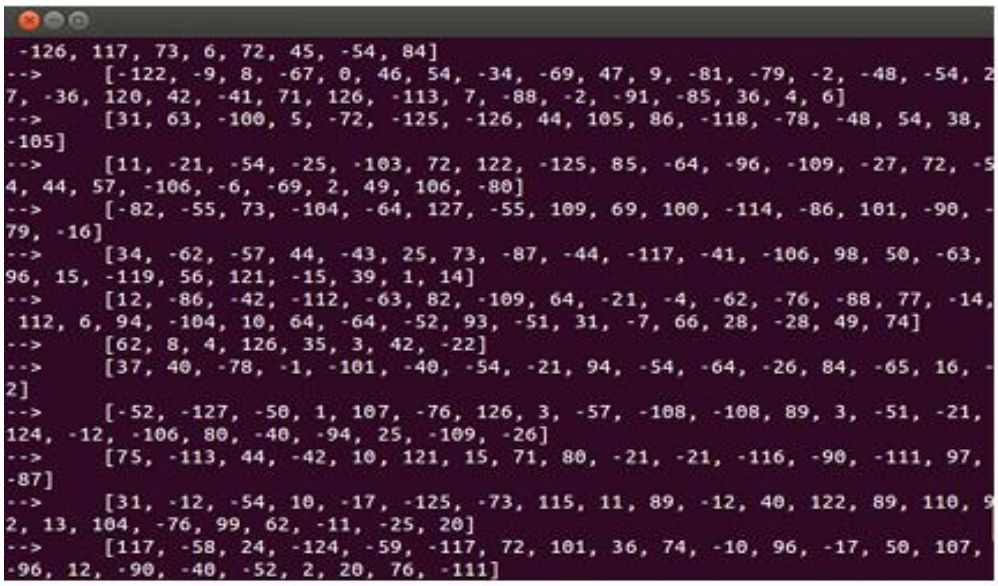

Figure 3. *Encrypted Output Data*

Comparison between Existing Work and Proposed Work

The key algorithm takes somewhat more time than RSA algorithm. In the event that we think about encryption of documents, at that point our proposed strategy emerges as it utilizes four remarkable prime numbers rather than two as in RSA algorithm. As the quantity of prime number is expanded, it will make the factorize it. Aside from that there is another common number each incorporated into both public key and private key. So the general security increments.

File Size (in Bytes)	Time Taken by Hadoop with out Encryption (in seconds)	Time Taken by Hadoop with Proposed Method (in seconds)	Diffrence (in s)
87040000	143	192	49
174080000	80	188	108
230400000	179	327	148
348160000	119	343	224
435200000	180	385	205
522240000	200	412	212
609280000	226	425	199

Table 1: *Comparison of proposed method and existing one*

Table 1 demonstrations how much time Hadoop takes to finish the doled out activity without utilizing any encryption plan and how much time it takes to finish the guide diminish work in the awaken of relating the proposed encryption scheme. The record size is appeared in no of bytes, the time taken by hadoop to finish the activity without encryption is determined in a moment or two, time taken by hadoop to finish the activity with our proposed encryption framework is determined in a moment or two and afterward the difference between these multiple times is taken.

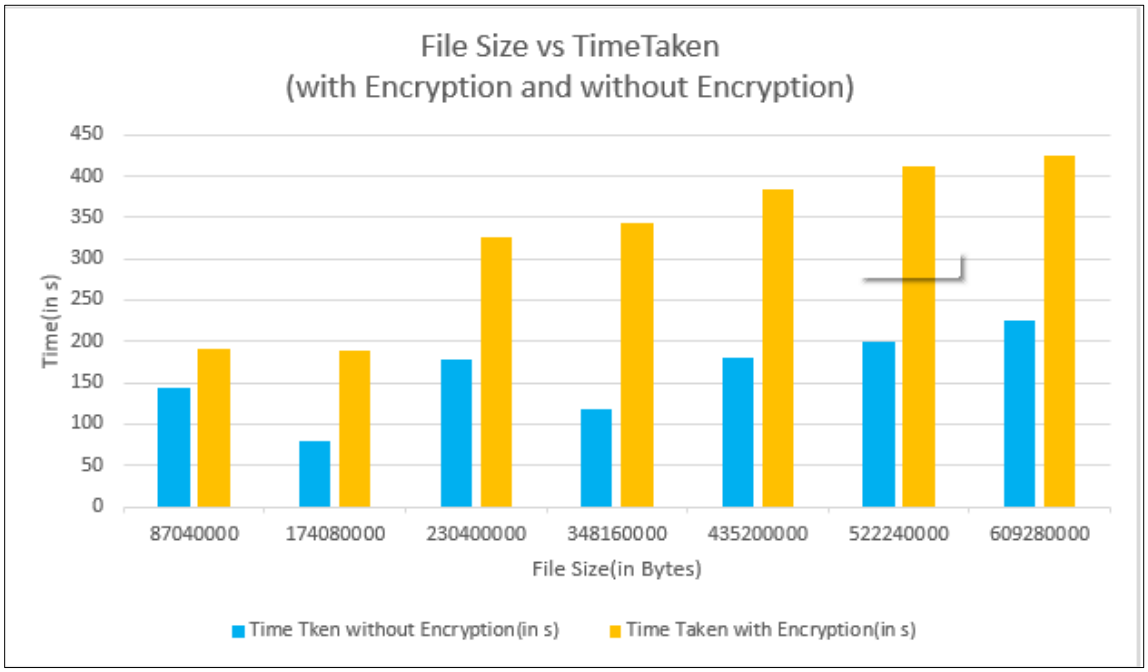

Figure 4: *File Size vs Time Taken (with and without Encryption)*

Figure 4 demonstrates the time taken to finish the activity increments in the event that we encryption on the documents before putting away it in HDFS yet when contrasted with the rate at which the record size is expanding, the time taken isn't expanding at that rate.

Conclusion

In this period of computerized world, information is expanding exponentially on regular routine which can't be taken care of by customary database the board framework. So as to manage such a gigantic measure of information offered ascend to the enormous information issue. Hadoop is a versatile technique to confront the difficulties brought about by enormous information. As the quantity of bytes composed by the MapReduce employment of Hadoop does not increment at a similar rate at which information is expanding, so Hadoop is an appropriate technique to defeat huge information issue. The Hadoop MapReduce structure over HDFS shows the abilities of cell phones to profit from the enduring development of enormous information in the portable environment. Our framework tends to each one of the requirements of information preparing in versatile cloud vitality effectiveness, information dependability and security.

REFERENCES

1. Ashish Ghosh, Aggregation pheromone density based data clustering, Information Sciences, 178(13): 2816-2831, 2008.
2. Atiya Parveen, Sobia Habib, Waseem Ahmad, The Cloud changing the Indian healthcare system, International Journal of Computer Science and Mobile Computing, IJCSMC, 2(5):238 -243, 2013.
3. B. T. Rao and L. S. S. Reddy, “Survey on Improved Scheduling in Hadoop MapReduce in Cloud Environments,” Int. J. Comput. Appl., vol. 34, no. 9, p. 5, Jul. 2011.
4. Babu, “Towards automatic optimization of MapReduce programs,” Proc. 1st ACM Symp. Cloud Comput. - SoCC ’10, p. 137, Jun. 2010.
5. C. L. Abad, Y. Lu, and R. H. Campbell, “DARE: Adaptive Data Replication for Efficient Cluster Scheduling,” in Cluster Computing (CLUSTER), 2011 IEEE International Conference on, 2011, pp. 159–168.
6. C. Li, H. Zhuang, K. Lu, M. Sun, J. Zhou, D. Dai, and X. Zhou, “An Adaptive Auto-configuration Tool for Hadoop,” in Engineering of Complex Computer Systems (ICECCS), 2014 19th International Conference on, 2014, pp. 69–72.
7. Du, S. and Chen, S. “Weighted support vector machine for classification”, IEEE International Conference on Systems, Man and Cybernetics, 4, 3866-3871.2005.
8. Dweepna Garg, Khushboo Trivedi, B.B.Panchal, "A Comparative study of Clustering Algorithms using MapReduce in Hadoop",International Journal ofEngineeringResearch & Technology (IJERT), Vol. 2 Issue 10, October - 2013.
9. Ekanayake et al., Twister: a runtime for iterative MapReduce, HPDC ’ 10 Proceedings of the 19th ACM International Symposium on High Performance Distributed Computing Pages 810-818, 2010.

10. Este, A.Gringoli F.and Salgarelli, L.“Support Vector Machines for TCP traffic classification”, Computer Networks, 53, 2476-2490. 2009.
11. Fayyad, U. M.; Piatetsky-Shapiro, G.; Smyth, P.; and Uthurusamy, R. Advances in Knowledge Discovery and Data Mining. Menlo Park, Calif.: AAAI Press. 1996.
12. Gemson Andrew Ebenezer J. and Durga S, "Big data analytics in healthcare: a survey", ARPN Journal of Engineering and Applied Sciences, 10(8), 2015.
13. He, W. Fang, Q. Luo, N. K. Govindaraju, and T. Wang, “Mars: a MapReduce framework on graphics processors,” in Proceedings of the 17th international conference on Parallel architectures and compilation techniques - PACT ’08, 2008, p. 260.
14. Isard, M. Budiu, Y. Yu, A. Birrell, and D. Fetterly, “Dryad: distributed data-parallel programs from sequential building blocks,” ACM SIGOPS Oper. Syst. Rev., vol. 41, no. 3, pp. 59–72, Mar. 2007.
15. J. Virajith, B. Hitesh, C. Paolo, K. Thomas, and R. Antony, “Bazaar: Enabling Predictable Performance in Datacenters,” 2012.
16. K. Kc and K. Anyanwu, “Scheduling Hadoop Jobs to Meet Deadlines,” in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010, pp. 388–392.