Security Implementation of Distributed Systems in Cloud Environment

S. Saisatyanarayana Reddy, M.A.Jabbar, N.Hanuman Reddy

Abstract: **This paper provides a framework of security in distributed systems in the cloud environment. Security for distributed system is one of the most important things that researchers need to take care of. Distributed systems also involve monetary transactions like ATM machines. If an ATM machine is corrupted intentionally, then the loss will be irreparable. Attackers may attack in any non recognized form. We build distributed systems so that the users will be connected with each other using information technology in a cost effective way. In this paper we are proposing a model of computer systems that will be distributive but the computer hardware will be completely abstracted from potential users. As the environment is cloud based, for developers this type of model will be cost effective. As security is concerned, there will be inbuilt security because of cloud environment. Our model is named as cloud secured communication algorithm (CSCA). This model provides a much better security than the existing algorithms.**

Index terms: **Distributed Systems, Cloud Computing, Security**

I. INTRODUCTION

Cloud environment is used to provide economy of scale. As hardware and data can be shared amongst different resources, the cost reduces. Cloud environment is the most wanted technology by all organization, but what remains as the matter of concern is security. Cloud and distributed systems can transfer data from one user to other through network. These network channels are always prone to malicious attack. These channels have to be protected. This was an eminent question in front of the researchers. By what means they will maintain data integrity. If they would segregate the data for the purpose of security, then all how would they get back the original data? Data authentication, privacy and authorization the researchers had to implement in the cloud and distributed environment. How would they implement all these? They also thought that it is the duty of the cloud service provider to ascertain data integrity. The cloud service providers should be capable of maintaining the internal working of cloud without exposing the details to the customers. It was the duty of the cloud service provider to provide authenticate data and provide correct data to the clients. It was also the client's duty to trust the cloud service provider. Cloud service provider should maintain isolation of data. Finally it was also important to understand to what extent, the administrators of this environment should be allowed to access the customer's data. Security in cloud computing is shared between the cloud service provider and the IT department. Some of the cloud services can be outsourced also. This makes it cost effective.

II. RELATED WORK

Cloud computing can implemented in various forms of environment. For example it can be implemented in parallel computing, clustered computing, distributed computing and so on and so forth. In case of parallel computing, a large task is divided into smaller unrelated tasks. In clustered computing, many independent systems can be connected with the help of a high speed network. In clustered environment, every system is independent and they give an illusion to the users that they have an independent system at their disposal [1,2,3,4].

In distributed computing, one system can share the hardware and the software. These systems may also have more than one storage unit. These system do not share memory, rather they communicate with each other by passing on messages asynchronously or synchronously. There were many reasons to shift towards distributed computing like larger jobs could be performed with the help of shared resources, rather than

S. Saisatyanarayana Reddy is with vardhaman college of Engineering, Hyderabad, India E mail : saisn90@gmail.com

M.A. Jabbar is with vardhaman college of Engineering, Hyderabad, India E mail: jabbar.meerja@gmail.com

N.Hanuman Reddy is with vardhaman college of Engineering, Hyderabad, India E mail: raju9009@gmail.com

independent system. Another reason was that any task could be performed remotely on vital dataset. These tasks can be very critical [5, 6, 7, 8].

Distributed computing is built upon many layers. The lowest layer being the network layer. This layer is responsible for making the terminals talk to each other. Upper layers can provide security services. Any distributed application runs on the topmost layer. The topmost layer can be broken into agents, objects and threads. All the terminals in distributed computing are capable of running different applications [9, 10,11].

Each of the process that runs in distributed environment comprises of more than one thread. These threads can work on their own or can also synchronize and work together. Each process may contain more than one object. Objects are data grouped together. They also contain method that can work on the data [12, 13].

Cloud computing is a way to provide secured on demand access to a pool of resources. Security is very important in cloud and distributed environment. There are various security algorithms that can be implemented. Researchers thought of various techniques like fragmentation of data. The main data was fragmented and was distributed in different channel. The main reason behind fragmentation was to separate the data so that malicious users cannot understand the actual data.

It was also required that the cloud service provider should not disclose the technicality to the clients. It was important on the user's part also to trust the cloud service provider. In case of cloud computing, all the data is stored in some specific platforms called datacenters. Datacenters keeps the data secured and private. It is also possible that security threat can occur at the time of implementing the cloud infrastructure. Any loophole in the infrastructure can be taken as an opportunity by the malicious users [14].

Cloud environment should provide data integrity and privacy. All the levels of the cloud layer should deal with security issues. Researchers can implement security with the help of existing cryptographic algorithms. Data should be encrypted and then sent through different channels. The encryption can be done with the help of any existing algorithms. Data should be decrypted in the other side and it should be collected correctly. Cloud service provider should also provide with confidentiality. It should be also seen that when data is transferred through the channels, there should not be any loss of data or leakage of data. There should be proper governance of data by the cloud service provider [15].

Cloud architecture plays certain roles that are always prone to attack. It is important to understand who is accessing the cloud. It is important to manage the user's identity and also it is necessary to encrypt the data for communication. Cloud architecture should maintain virtualization of service.

Some network problem might be associated that might be a problem in the code.

III. PROPOSED WORK

The propose work firstly implements a distributed model of computing systems in a cloud environment. The cloud environment abstracts the hardware details from the end users. This is a big advantage to the vendors as they can outsource the task of the hardware to other parties. Though there are some inherent disadvantages like cloud reliability issues, latency, congestion etc. As these disadvantages are minor, they can be ignored for the time being. Secondly the proposed system implements a security model called as CSCA (Cloud secured communication algorithm).

The proposed algorithm has two parts. The first part considers "n" points on the (x, y) plane. Then we consider a polynomial k(x) such that y=k(x) for each of the "n' points. Then we can show how to disperse data M into t pieces such that and then we can get back the data again with the knowledge of t pieces. We are assuming that when we are in the process of rebuilding data, remaining (t-1) piece does not disclose information about the data M. We are implementing this system using the existing principles of cryptography that uses public and private key mechanisms. These keys are very robust and not easily detectable.

These M data are divided into P channels to obtain parallelism. This bifurcation of data provides more security. Before transferring the data, we will know the details of the sender and the receiver. We will be concentrating on the servers, the storage server and the processing server. We will be fragmenting the original data into all the available channels. This provides additional security. There will be back up of data in the storage server. Cloud will be collecting back these data based on the existing knowledge of P channels. Before sending the fragmented data into P channels, we need to encrypt them. The encryption maybe done with any existing algorithm of Cryptography. In order to get the actual data the attacker has to go through all the channels. This imposes difficulty for the attacker.

This technique does not allow denial of service attack. There will be no threat of data replication.

.

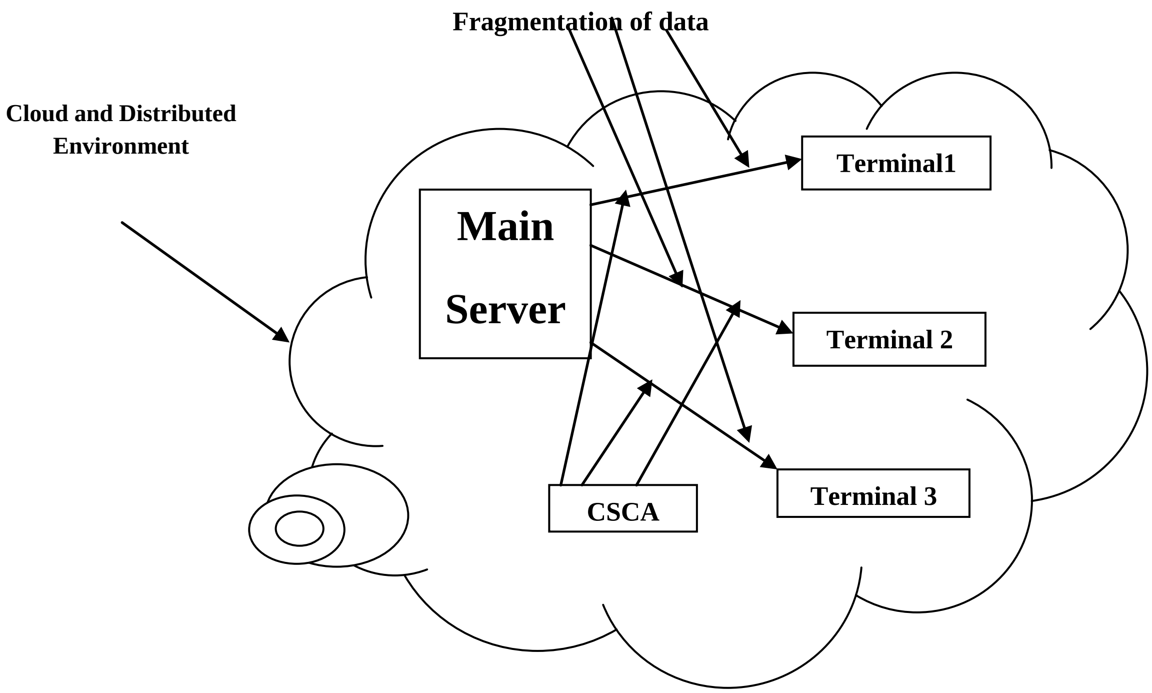

Fig 1: Cloud Secured Communication Algorithm

IV. RESULT ANALYSIS

We can do a comparison between the existing model and our proposed model by analyzing certain parameters like average time of failures in 50 seconds. We find that

1. In each 50 second, one server stops working
2. In each 50 second, two servers stop working
3. In each 50 seconds, three servers stop working

We use simulation for each of the above cases with fragmentation number equal to 20. The simulation period will be for half an hour. We calculate the recovery efficiency using the formula

RE= maximum data size/ mean time to repair

When we compare the recovery efficiency of existing model with our proposed model, we find the RE is higher for our model.

V. CONCLUSION

This paper proposes a model that implements distributed system in cloud environment. These kinds of framework provide advantages to the vendors as they are cost effective. Distributed systems are very fast as they allow users to connect with each other using information technology. Cloud environment hides all the physical level details from the end users. Though there are certain disadvantages like network congestion, latency etc. But these disadvantages are very minor and they can be easily ignored. For security sake we are fragmenting the data into channels.

These channels are secured and data is not concentrated in one place. Attackers need to search so many channels to get the original data back. This might be time consuming for the attacker. Before transferring the data into channels, the fragments are encrypted by any of the existing cryptographic algorithm. We will be choosing the most robust cryptographic algorithm. The attackers will have difficult time to decrypt the data.

The proposed model does not allow denial of service attack. Cloud environment itself provides some basic security. These security services are inherent to cloud environment.

REFERENCES

[1] Vic (J.R) Winkler. Securing the cloud - cloud Computer Security Techniques and Tactics. Elsevier Inc, 2011.

[2] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani. Towards secure mobile cloud computing: A survey. Future Generation Computer Systems (2012), doi:10.1016/j.future.2012.08.003.

[3] J. Sinduja, S. Prathiba. Modified Security FrameWork for PIR cloud Computing Environment. International Journal of Computer Science andMobile Computing-2013.

[4] Clara Leonard. PRISM : la NSA argumente, le Guardian fait de nouvelles rev´ elations ´ . From http://www.zdnet.fr/actualites/prism-lansaargumente-le-guardian-fait-de-nouvelles-revelations-39791924.htm. ZDNet, Jun 28,.2013. consulted Nov 20, 2013.

[5] Glenn Greenwald, Ewen MacAskill, Laura Poitras. Edward Snowden: the whistleblower behind the NSA surveillance revelations. http://www.theguardian.com/world/2013/jun/09/edwardsnowdennsa-whistleblower-surveillance. The Guardian, jun 10,2013.

[6] Almokhtar Ait El Mrabti, Anas Abou El Kalam, Abdellah Ait Ouahman. Data Security In The Multi-Cloud. The International Conference On Networked Systems May 2-4, 2013, Marrakech, Morocco. The First International Workshop on Security Policies in cloud Environment (PoliCE2013)

[7] Keiko Hashizume, David G Rosado, Eduardo Fernndez-Medina, Eduardo B Fernandez. An analysis of security issues for cloud computing. Hashizume et al. Journal of Internet Services and Applications. SpringerOpen Journal. 2013, 4:5

[8] A.B. Chougule, G.A. Patil. Implementation and Analysis of EFRS Technique for Intrusion Tolerance in Distributed Systems. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[9] P. Mell and T. Grance. The NIST definition of cloud computing. Special Publication 800-145. Retrieved September 2011, from http://csrc.nist.gov/publications/PubsSPs.html.

[10] Joshna S, Manjula P. Challenges and Security Issues in cloud Computing. International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 558-563.

[11] Rajkumar Buyya, James Broberg, Andrzej M.Goscinski. Cloud Computing: Principles and Paradigms. John Wiley & Sons, 17 dc. 2010.

[12] K. Sudha, M.Tech. MISTE, B. Anusuya, P.Nivedha, A. Kokila. A Survey on Encrypted Data Retrieval in cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 5, Issue 1, January 2015.

[13] Almokhtar Ait El Mrabti, Anas Abou El Kalam, Abdellah Ait Ouahman. Les defis de s ´ ecurit ´ e dans le cloud Computing - Probl ´ emes et solutions ` de la securit ´ e en cloud Computing ´ . 2012 National Days of Network Security and Systems, IEEE Catalog Number CFP1239S-PRT

[14] Wenjun Luo, Guojing Bai, Ensuring the data integrity in cloud data storage. International Conference on cloud Computing and Intelligence Systems (CCIS), IEEE,240 243,15-17, 2011.

[15] Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, Shvetank Verma, Vijay K. Chaurasiya, Rahul Gupta. An architecture based on proactive model for security in cloud computing. IEEE 2011