ISSN: 2321-7782 (Online)
Volume 4, Issue 2, February 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Implement PACK with AES in cloud Computing

Amavi A. Vispute[1]
Computer Science & Engineering
JSCOE, Hadapsar
Pune - India

Prof. H. A. Hingoliwala[2]
Computer Science & Engineering
JSCOE, Hadapsar
Pune - India

Abstract: ***In this paper, we use concept of PACK (predictive ACKs), which act like a traffic redundancy elimination (TRE) system, Designed for cloud computing customers. TRE is designed on cloud to reduce traffic as well as cost regarding TRE Computation and storage will be optimized. The main advantage of the Pack Cloud-server is its ability to span end clients TRE effort, thus minimizing processing costs prompted by the TRE Algorithm. Unlike previous solutions Pack does not require server to continuously keep track on customer to maintain the status of the server. Pack maintain computing environment that combine server and client movement to maintain cloud elasticity. Pack is based on TRE technology; TRE is used to eliminate the transmission of redundant content as well as allow client to use newly received chunk to identify previously received chunks chains, which in turn can be used as reliable predictors future transmitted chunks. In our proposed work we are using encryption concept. We will send the chunks in encrypted format. For encryption we are using AES algorithm which is based on symmetric block cipher. This is using for security Purpose. We are going to secure our file from other traffics.***

Keywords: cloud computing; Traffic Redundancy Elimination; Predictive Acks; Network optimization; Secure Hash Algorithm-1; Advanced Encryption standard.

I. INTRODUCTION

Cloud computing offers its customers an economical and convenient *pay-as-you-go* service model, known also as *usage-based pricing* [1]. Cloud customers1 pay only for the actual use of computing resources, storage, and bandwidth, according to their changing needs, utilizing the cloud's scalable and elastic computational capabilities. In particular, data transfer costs (i.e., bandwidth) is an important issue when trying to minimize costs. In cloud computing Environment, Cloud customers pay only for the actual use of computing resources, storage, and bandwidth, according to their changing needs, utilizing the clouds scalable and elastic computational capabilities. Cloud customers, applying a judicious use of the clouds resources, are motivated to use various traffic reduction techniques, in particular traffic redundancy elimination (TRE)[1], for reducing bandwidth costs.

To the best of our knowledge, no one previous works have been addressed the requirement for cloud computing-friendly, end-to-end TRE[2] which form PACK. TRE is used to eliminate unnecessary transmission of content and, therefore, Important to reduce network costs. Current End-To-End solution is sender based here cloud load balancing and optimization done on server side which requires full synchronization between client and server. But there is lack of synchronization so lose efficiency. Most of its computational efforts on cloud side so less cost-effective. We have presented pack, a receiver-based, Cloud-friendly, end-to-End TRE that is based on speculative fiction the theory is that the latency and reduce operating costs to maintain a consistent Server pack required Customer status thus enabling cloud elasticity and mobility, While long-term redundancy protection.

In the proposed system, for provide much more security over network ,we will apply data integrity verification by using hashing algorithm like SHA-1and also provide encryption/decryption using symmetric algorithm like AES[3] .AES is a

symmetric block cipher it uses same key for both encryption and Decryption We are going to secure our file/data from unauthorized access.

II. LITERATURE SURVEY

A. *Low-bandwidth Network File System(LBFS)*

Benjie chen and and David Mazieres are proposed[4] LBFS which is a network file system that saves bandwidth by taking advantage of commonality between files. LBFS breaks files into chunks based on contents, using the value of a hash function. It indexes file chunks by their hash values. Under common operations such as editing documents and compiling software, LBFS can consume over an order of magnitude less bandwidth than traditional file systems. Such a dramatic savings in bandwidth makes LBFS practical for situations where other file systems cannot be used. Advantages of LBFS are it avoids sending redundant data, Require magnitude less bandwidth and indexing help to reduce redundancy. Disadvantage is not suitable for application which require very High bandwidth.Eg.video, 3D video etc.

B. *SmartRE*

K. C. Lan and C. M. Chou invent a SmartRE[5] is An Architecture for Coordinated Network-wide Redundancy Elimination. It provides a naive link-by-link view and adopts a network-wide coordinated approach. It is suitable for handling heterogeneous resource constraints and traffic patterns and for incremental deployment. Smart RE is naturally suited to handle heterogeneous resource constraints and traffic patterns and for incremental deployment. They address several practical issues in the design to ensure correctness of operation in the presence of network dynamics. Across a wide range of evaluation scenarios, Smart RE provides 4-5 improvement over nave solutions and achieves 80-90 of the performance of an ideal, unconstrained RE network-wide alternative. They address several practical issues in the design to ensure correctness of operation in the presence of network dynamics.Advantages are it enable more effective utilization of the available resources at network devices, can apply to Datacenter and MultiHop wireless network .Disadvantage is It having designing problem in Dynamic network model.

C. *EndRE: An End-System Redundancy Elimination Service for Enterprises[6]*

Using extensive traces of enterprise network traffic and testbed experiments, they show that our end-host based redundancy elimination service, EndRE, provides average bandwidth gains of 26 and, in conjunction with DOT, the savings approach that provided by a WAN optimizer. Further, EndRE achieves speeds of 1.5-4Gbps, provides latency savings of up to 30 and translates bandwidth savings into comparable energy savings on mobile smart phones. In order to achieve these benefits, EndRE utilizes memory and CPU resources of end systems. For enterprise clients, we show that median memory requirements for EndRE are only 60MB. At the server end, they design mechanisms for working with reduced memory and adapting to CPU load.

D. *SHA-1*

In base paper[1], SHA-1 operation is performed along with data while transfer in between communication.SHA-1[7] is a cryptographic hash function. SHA-1 produces a 160-bit (20-byte) hash value. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. SHA-1 produces a message digest. But its not more secure.it has lots of drawbacks.

E. *AES*

AES stands for the Advanced Encryption Standard is a symmetric block algorithm. This means that it takes 16 byte blocks and encrypts them. It is "symmetric" because the key allows for both encryption and decryption. Following are objective which is provided by AES algorithm[3]:

1. Resistance against all known attack

2. Speed and Code Compactness on a wide range of platform

3. Single key is used for encryption/decryption purposes.

4. Creating secure cloud architecture.

5. Block size and Key size can vary making algorithm versatile.

6. Easy to implement

7. Failure detection and prediction.

8. Secure management of virtualized resource.

9. Time required checking all the possible keys at 50 billion keys per second

III. PROPOSED SYSTEM

Problem Definition:-To provide more secure communication in network traffic over cloud.for provide much more security over network ,we will apply data integrity verification by using hashing algorithm like SHA-1and also provide encryption/decryption using symmetric algorithm like AES.

AES[3] is a symmetric block cipher it uses same key for both encryption and Decryption We are going to secure our file/data from unauthorized access.When encryption and Decryption performed then chunk size will be reduced so that it may reduce bandwidth cost and also required less buffered storage space.We are using encryption and Decryption technique for security purpose and in existing system we use SHA-1 algorithm which is not much resistance against attacker like Brute-force attack so we are using AES algorithm which having more resistance power to face attack over network.

PACK Algorithm along with (AES Cryptographic algorithm)

Following is step that shows how algorithm works

1. At PACK receiver side, stream of data received which is parse in sequence of variable size.
2. Chunks are then compared to receiver local storage also called chunk store. If matching chunk is found in local chunk store, receiver retrieves sequence of chunk referred as chain which follows LRU scheduling.
3. Using constructed scheduling, receiver send prediction to sender for subsequent data. Prediction sent by receiver includes predicted data, hint and signature of chunk.
4. Sender identifies predicted range in its buffered data and verifies Hint for range, if result matches the received Hint, it continue to perform the more computationally SHA-1 signature operation.
5. Upon signature match sender send a confirmation message to receiver.

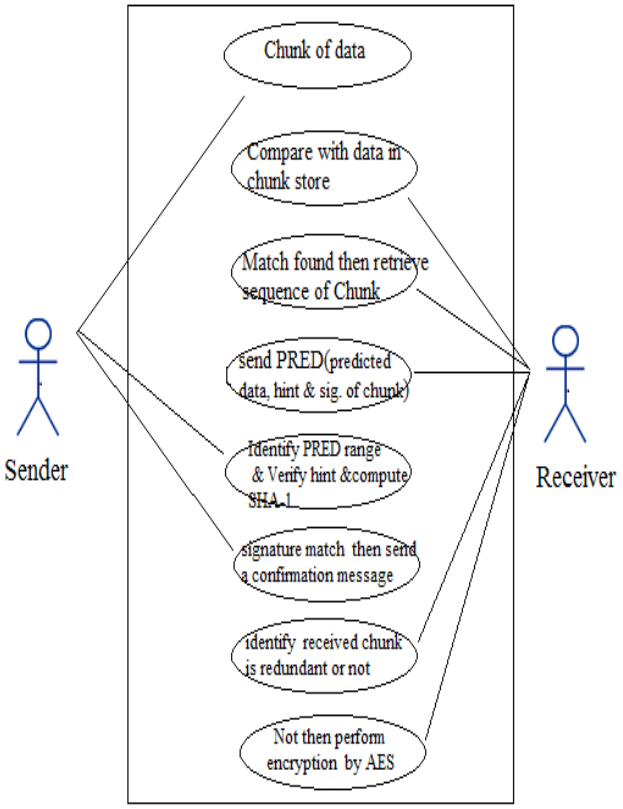

Fig. 1 working of PACK algorithm along with AES

IV. Architecture of Proposed System Model

In system architecture of the Secure_PACK, After the non redundant data is being identified, the data is encrypted using the AES algorithm and is sent to the cloud server for storage. Since in cloud computing a distributed computing takes place, it is not secure to place the raw data in the cloud. Hence for maintaining security, data is encrypted using AES. Thus specific data owner can only view his data, which created privacy. In the previous work, even though bandwidth and cost were reduced, security level was not at all maintained. In our work the security level is maintained thus this overcomes the disadvantage of the existing system.

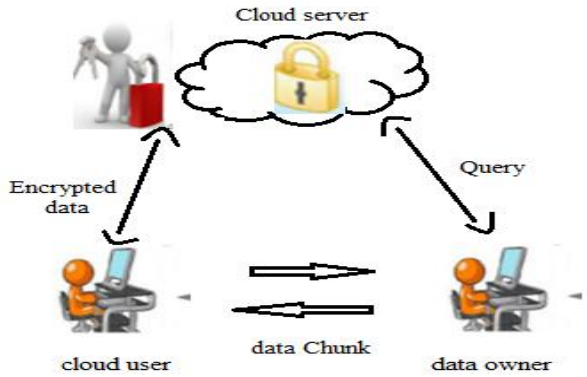

Fig. 2 Overall Architecture of PACK algorithm

V. Conclusion

The Traffic redundancy eliminate over network.TRE is also used to Proprietary middle box solution inadequate that reduces a growing cloudy needs is operational the cost accounting application latencies, while user dynamics, and elasticity. The main advantage of the Pack Cloud-server is its ability to span end clients TRE effort, thus minimizing processing costs prompted by the PACK Algorithm Limitations is that there is a security problem while sending a data in chunk for over a network so for solving this problem AES cryptographic algorithm which provide much more security against attacker. AES

cryptographic algorithm is used. The encrypted data is maintained in the cloud, thus this provides much more security to the previously existing system. Hence a secure, cost efficient and with reduced bandwidth cloud system will be obtained.

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Prof. H. A. Hingoliwala for his exemplary guidance, monitoring and constant encouragement which helped me in completing this task through various stages. The blessings, help and guidance given by his time to time shall carry me a long way in the journey of life on which I am about to embark.

References

1. E. Zohar, I. Cidon, and O. Mokryn, The power of prediction: Cloud bandwidth and cost reduction, in Proc. SIGCOMM, 2011, pp. 8697.
2. N. T. Spring and D. Wetherall, A protocol-independent technique for eliminating redundant network traffic, in Proc. SIGCOMM, 2000, vol. 30, pp. 8795.
3. Abha Sachdev,Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm," in Proc. International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013 19
4. A. Muthitacharoen, B. Chen, and D. Mazières, "A low-bandwidth network file system," in *Proc. SOSP*, 2001, pp. 174–187.
5. K. C. Lan and C. M. Chou, SmartRE: An Architecture for Coordinated Network-wide Redundancy Elimination M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.
6. R. EBhavish Aggarwal, Aditya Akella, Ashok Anand, Athula Balachandran, Pushkar Chitnis, Chitra Muthukrishnan, Ramachandran Ramje and George Varghese, EndRE: An End-System Redundancy Elimination Service for Enterprises..
7. http://en.wikipedia.org/wiki/SHA1.

