

Predictive ACKs along with AES in cloud computing

Miss Amavi A. Vispute : Prof.H.A.Hingoliwala

Department of Computer Engineering : Department of Computer Engineering

J.S.C.O.E. Hadapsar, Pune University, : J.S.C.O.E. Hadapsar, Pune University,

Maharashtra. : Maharashtra

E-mail: amuvispute@gmail.com ; ali_hyderi@yahoo.com

ABSTRACT

In this paper, we used PAK (predictive ACKs), which act like a traffic redundancy elimination (TRE) system. TRE is used to reduce traffic cost regarding TRE Computation and storage will be optimized. Elasticity is maintained by computing environment that combine server and client movement. TRE is used to eliminate the transmission of redundant content and 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 will provide data integrity, Confidentiality, verification by using hashing algorithm like SHA1 and also provide encryption and decryption using symmetric algorithm like AES. The non redundant data is identified and using AES those data chunks are encrypted and sent to the cloud for storage. Use of AES enhance security. By using this AES algorithm, the customer services can become quiet secured and which can help in further enhancement of the cloud computing standards.

Keywords: Traffic Redundancy Elimination; Predictive Acks; Secure Hash Algorithm 1; Advanced Encryption standard.

1. INTRODUCTION

In cloud computing, TRE[2] is used to eliminate unnecessary transmission of content and, therefore, Important to reduce network costs. Current End-To-End solution are sender based here cloud load balancing and optimization done on server side which require 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. cloud customers,

applying a judicious use of the clouds resources, are motivated to use various traffic reduction techniques, in particular traffic redundancy elimination (TRE), for reducing bandwidth costs.

In the proposed system, for provide much more security over network, we will apply data integrity verification by using hashing algorithm like SHA-1 and 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.

Following are objective which is provided by AES algorithm[4]:

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 to check all the possible keys at 50 billion keys per second.

2. LITERATURE SURVEY

2.1 A Low-bandwidth Network File

System(LBFS)

Benjie chen and David Mazieres are proposed[5] LBFS which is a network file system that saves bandwidth by taking advantage of commonality between files. LBFS 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 on small regions of the file to determine chunk boundaries. It indexes file chunks by their hash values, and subsequently looks up chunks to reconstruct files that contain the same data without sending that data over the network. 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.

2.2 SmartRE

K. C. Lan and C. M. Chou invent a SmartRE [6] 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. 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.

2.3 A Redundancy in Network Traffic: Findings and Implications

Ashok Anand, Chitra Muthukrishnan, Aditya Akella and Ramachandran Ramjee[7] found out the

various issues in network design while thinking about redundancy elimination. Despite the increasingly important role of redundancy elimination in the network infrastructure, very little is known about the range of benefits and tradeoffs these approaches offer today, and the fundamental issues underlying their design. Using packet traces collected at twelve distinct network vantage points, they showed that packet-level redundancy elimination techniques can deliver average bandwidth savings of 15-60 for enterprise and university access link as well as the links connecting busy web servers.

Advantages:are 75-90 percent middlebox bandwidth saving, Improve effective bandwidth of n/w access link of datacenter, Redndncy in n/w packet can eliminated.

Disadvantage: Enterprise traffic was not reduced peak and traffic periods was variable.

2.4 SHA-1

SHA-1 operation is performed along with data while transfer in between communication.SHA-1[8] 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.

3. SYSTEM ARCHITECTURE

Problem Definition:- To provide more secure communication in network traffic over cloud.

In proposed system model, we have provided more security by using AES [9] algorithm when encryption and decryption is performed on data. 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.In our system, encrypt a message using AES and then send along a SHA1 hash of the unencrypted message so that when the message was decrypted they were able to validate the data.

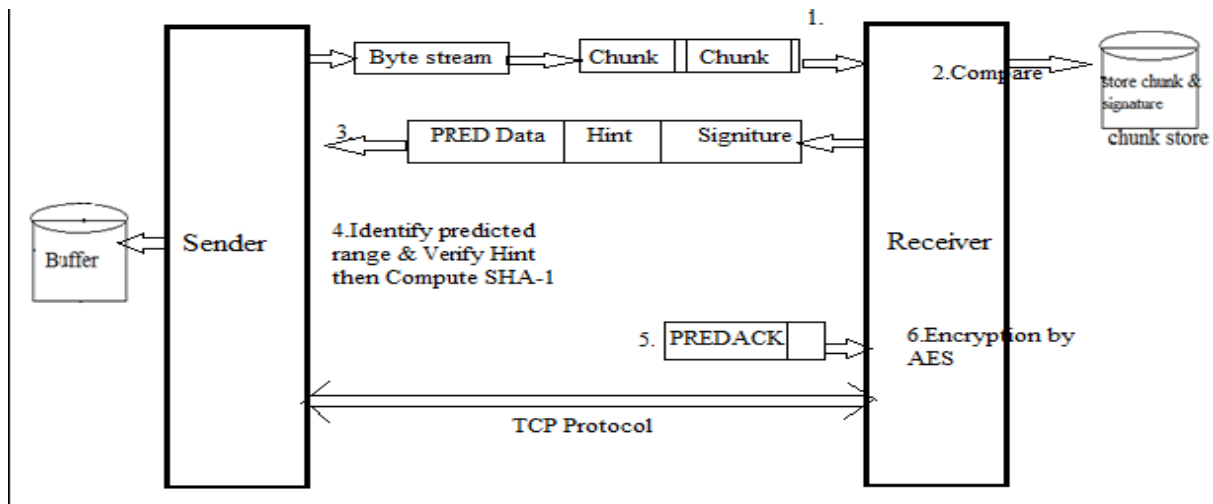


Fig 1: Overall Working of PACK with AES.

4. PROPOSED SYSTEM MODEL

Following are objective which is provided by AES algorithm:

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. It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits).
6. Failure detection and prediction.
7. Secure management of virtualized resource.

PACK Algorithm along with (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. chunk 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 follow LRU scheduling.
3. Using constructed scheduling, receiver send prediction to sender for subsequent data .Prediction sent by receiver include 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, thus permitting it to copy the matched data from its chunk store.
6. Receiver identify that received chunk is redundant or not ,if not then perform encryption on data by AES and sent to cloud server.

In this message transmission TCP wire protocol is used which provide consistency in communication. for making more secure transmission AES cryptographic algorithm may apply so that transmission become more secure against attacker.

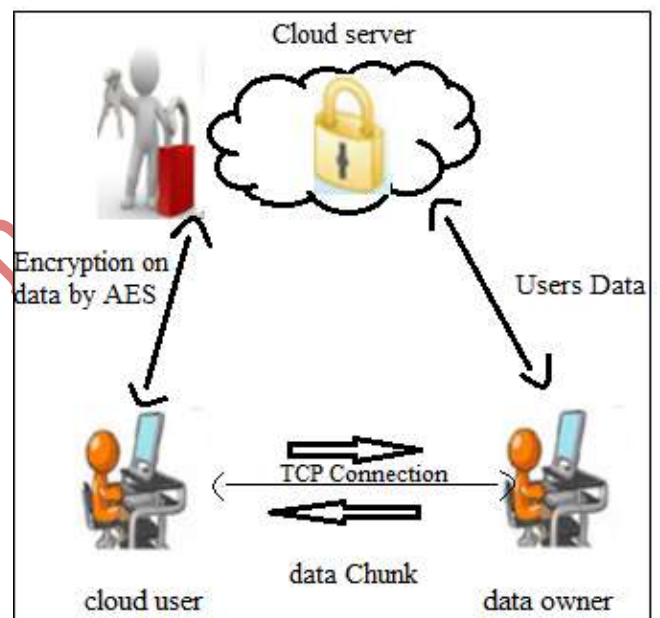


Fig 2: Encrypted data by AES in Cloud server.

5. MATHEMATICAL MODELING AND ALGORITHM

Let S be the set {I, O, P, F, S} where,

- I : Input set
- O: Output set
- P: Process set
- F: Failure cases
- S: Successful cases

In our paper,

- 1) Input set I = Set of chunk{ch1,ch2,..ch-n}

ch1=a block of file
ch2=a block of file
ch-n= a block of file

- 2) Output set O = {Encrypted data/File}

- 3) Process set: P = {P1, P2, P3, P4, P5}

P1= Arrival of no. of chunks:

First new data is received by receiver in the form of chunk.

P2=Compare received chunk.

chunk 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 follow LRU scheduling.

P3= send prediction to sender.

prediction =(S U L U Sig)

S=Starting point in the byte stream,

L=Total length of the chunk

Sig=Identity of subsequent chunks

P4= identifies predicted range in its buffered data.

verifies Hint for range, If result matches the received Hint, it continue to perform the more computationally SHA-1 signature operation.

P5= signature match sender send PREDACK

P6= perform encryption on data by AES

AES[10] operates on blocks that are 128-bits in length.

The permissible key lengths are 128, 192, and 256 bits.

AES encrypts a 16-byte block using a 16-byte key with 10 encryption rounds.

Following details express AES Algorithm in mathematical form,

- The input to the AES round function can be viewed as a rectangular array of bytes or, equivalently, as a column vector of bytes, known as the state. In the AES, each byte is regarded as an element of the field. where $f(x) \in F_2[x]$ is the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. The AES specification defines a round in terms of the following three transformations:

- The AES S-Box. This is the only non-linear operation of the cipher. The value of each byte in the array is substituted according to a table look-up. This table look-up is the combination of three transformations:

- The input w is mapped to $x = w^{-1}$, where w^{-1} is defined by

$$w^{-1} = w^{254} = \begin{cases} w^{-1} & w \neq 0 \\ 0 & w = 0 \end{cases}$$

Thus the "AES inversion" is identical to the standard field inversion in K for non-zero field elements, with $0^{-1} = 0$.

- The intermediate value x is regarded as a F_2 -vector of dimension 8 and transformed using an (8×8) F_2 -matrix LA . The transformed vector $LA \cdot x$ is then regarded in the natural way as an element of K .

- The output of the AES S-Box is $(LA \cdot x) + d$, where d is a constant element of K

- The AES linear diffusion (mixing) layer.

- Each row of the array is rotated by a certain number of byte positions. This operation is called ShiftRow.

- Each column y of the array is considered as a vector of K^4 , and is transformed into the column $C \cdot y$, where C is a (4×4) K -matrix. This operation is called MixColumn.

- The AES subkey addition.

Before encryption, the original key is expanded into 11 round subkeys, each having 16 bytes. Then Following

the diffusion layer, each byte of the array is added (in K) to a byte from the corresponding array of round subkeys.

Receiver identify that received chunk is redundant or not, if not then perform encryption on data by AES and sent to cloud server.

4) Set F: Failure cases

The system is not able to work in less memory storage.

System also may not detect noise while transmission of data in block form.

5) Set S: Success cases

The system is able to provide secure distribution of data.

NP Complete: The problem of secure transmission of data over cloud traffic by using AES technique along with SHA-1 on data/file is NP-Complete, since proposed system i.e. PACK along with AES is satisfying secure, cost efficient and reduced bandwidth distribution of data in cloud computing.

6. A EXPERIMENTAL SETUP & RESULT ANALYSIS

A. Software tools used

- Operating system : Windows XP/7.
- Coding Language : JAVA/J2EE.
- IDE : Netbeans 7.4.
- Database : MYSQL.

B. Performance Analysis

In this section, we analyze the performance of our technique by comparing with previous[1] only PACK concept in terms of storage overhead & computation efficiency and security level.

A. Storage Overhead

We are identifying redundant chunk in chunk store and if redundant chunks are already present then we will remove the chunks or file. so in this way we are reducing storage overhead.

B. computation efficiency

We have used AES algorithm for computation so by using AES algorithm, the time required to check all the possible keys at 50 billion keys per second. This perform computational operation on very fast speed which also helps to reduce computational cost.

c. Security level

In our proposed work we used AES which is one of the secured algorithm among all cryptographic technique. It Resist against all known attack like brute force attack. Block size 128 bit and Key size 128,192,256 bit can vary making algorithm versatile and there is no weak key present for vulnerability.

The AES and SHA-1 are used to show the experimental results. The fig. 3 shows that security level increases even when the number of redundant chunk increases. The blue line shows the performance of the system when SHA-1 alone is applied. The red line shows the performance of the system when AES is used. In the proposed system

AES is being used for encrypting the data, hence security is maintained compared to the existing system. It clearly shows that the proposed system performs better than the previous methods in terms of security level.

Table 1. Comparison of Result analysis in between PACK and PACK with AES

Sr. No	Technique	Storage overhead	Computational efficiency	Security
1	PACK	Low	Low	Easily broken by Brute Forced Attack
2	PACK with AES	very Low	very high	Could not broken by Brute Forced Attack



Fig. 3. Experimental Result

Following bar chart shows number of redundant files and no redundant files over the network.

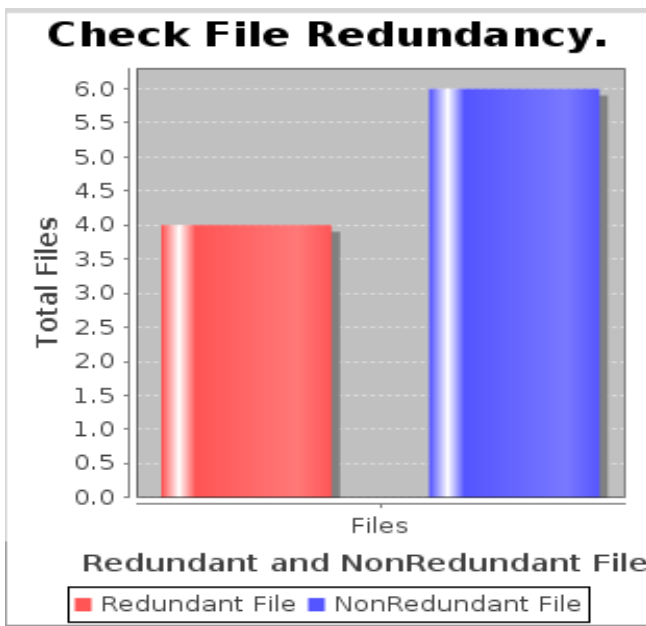


Fig. 4. Number of redundant files and no redundant files out of total files

Below Table 1 shows the comparison of Result analysis of previous method PACK and proposed method PACK with AES.

7. CONCLUSION

Predictive Acknowledgement is a receiver based TRE scheme which reduces them computation time and the cloud operational cost. The Traffic redundancy eliminate over network. TRE is also used to Proprietary middle box solution inadequate that reduces a growing cloudy needs. 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. Limitation 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 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.

8. 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.

9. REFERENCES

- [1]. I. E. Zohar, I. Cidon, and O. Mokryn, The power of prediction: Cloud bandwidth and cost reduction, in Proc. SIGCOMM, 2011, pp. 8697.
- [2]. Eyal Zohar, Israel Cidon, and Osnat Mokryn, PACK: Prediction-Based Cloud Bandwidth and Cost Reduction System, IEEE/acm transactions on networking, vol. 22, no. 1, february 2014
- [3]. Manpreet Kaur M.TECH. (CSE) LLRIET, Moga, Rajbir Singh Associate Prof. Head Department of IT, LLRIET, Moga, Implementing

- Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing, in International Journal of Computer Applications (0975 8887) Volume 70 No.18, May 2013.
- [4]. 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.
- [5]. A. Muthitachoen, B. Chen, and D. Mazires, A low-bandwidth network file system, in Proc. SOSP, 2001, pp. 174187.
- [6]. K. C. Lan and C. M. Chou, SmartRE: An Architecture for Coordinated Network-wide Redundancy Elimination in *Proc. SIGCOMM*, 2009, vol. 39, pp. 87–98.
- [7]. Suresh Chougala, Sharavana K Survey on, Traffic Redundancy and Elimination Approach for Reducing Cloud Bandwidth and Costs.
- [8]. <http://en.wikipedia.org/wiki/SHA1>
- [9]. Avi Kak (kak@purdue.edu), AES: The Advanced Encryption Standard, May 1, 2015.

IJournals