A Proxy Detection Techniques Used in Key Update for Cloud Computing

[1]Nitin Kumar Sahu,[2]Asst. Prof Anuj Kumar Pal,
[1]Research Scholar,[2]Assistant Professor
[1]Department of Computer Science and Engineering,
[1]Bansal Institute of Research and Technology, Bhopal ,India

Abstract : Cloud achievement may be a momentum mechanical progression within the making ready field during which typically turned around sketching out of organizations which might tend to the purchasers in indistinguishable course from the central utilities like sustenance, water, gas, power, and correspondence. Cloud or Distributed storage administrations have clad to be increasingly accepted. Visible of the importance of security, several Cloud storage encoding plans are projected to defend info from the people World Health Organization does not approach. In Existing framework, there is following partner problems that ar broken away at our projected work AES-256 is extremely traditional and effectively accessible for software engineer action within the event that it need to interrupt. Passing ordered info structure is not taken within the Existing framework. during this paper we tend to ar utilizing a being SHA-2 calculation for message key age and for info encoding utilized upgraded Bluefish calculation when the finished of this procedure we tend to to boot discover the negotiate server in cloud framework. For replica we tend to utilized cloudsim a java primarily based check system.

IndexTerms **- Cloud Computing, Cloud Security, Security issues**

I. INTRODUCTION

Distributed or cloud computing worldview has seen immense move towards its appropriation and it's changed into a pattern within the information innovation area because it guarantees huge price decreases and new business potential to its uses and suppliers. Cloud reckoning, as another innovation worldview with promising more, is completing more and higher glorious of late. It will provide purchasers infinite reckoning quality. Ventures and people will re-appropriate tedious calculation outstanding tasks at hand to cloud while not disbursal the extra capital on conveyance of title and maintaining instrumentality and programming. Lately, re-appropriating calculation has force in a lot of thought and been inquired regarding typically. it's been thought-about in varied applications as well as logical calculations. Software package as Service (SaaS) Platform as Service (PaaS) Infrastructure as Service (IaaS) IaaS-: Network, process Storage PaaS-: client gets associate open plateform/Solution SaaS-: client will Run Application in cloud Figure: one Cloud Service Models to attain this goal, however, it should meet many new needs.

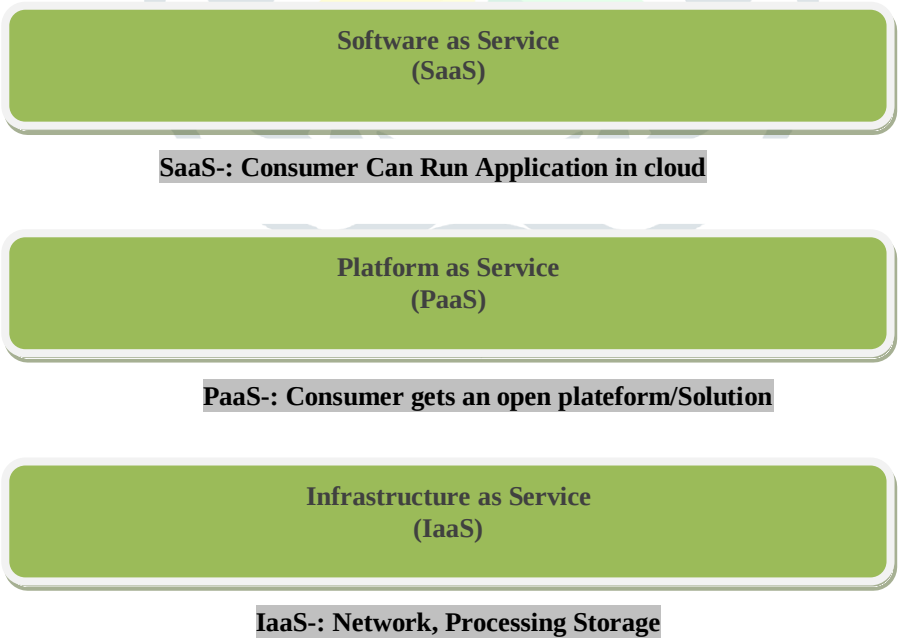

Figure: 1 Cloud Service Models

To achieve this goal, however, it must meet several new requirements. First, the authorized party that performs outsourcing computation for key updates should not know the real client's secret keys for cloud storage auditing. Otherwise, the new security threat will come. The authorized party should therefore only have an encrypted version of the cloud storage audit secret key of the user.

II. RELATED WORK

Jia Yu et al. **"Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates"**

In this paradigm, key updates can be safely outsourced to some authorized party, and thus the key-update burden on the client will be kept minimal. Specifically, we leverage the third party auditor (TPA) in many existing public auditing designs, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's secret key, while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also equips the client with capability to further verify the validity of the encrypted secret keys provided by TPA.

Chanying Huang et al**. "Efficient anonymous attribute-based encryption with access policy hidden for cloud computing"**

Using the idea of Boolean equivalent transformation, the proposed scheme can achieve fast encryption and protect the privacy for both data owner and legitimate access user. In addition, the proposed scheme can satisfy constant secret key length and reasonable size of cipher text requirements. We conduct theoretical security analysis, and carry out experiments to prove that the proposed scheme has good performance in terms of computational, communication and storage overheads.

Akhilesh Yadav et al. **"Securing Cloud Computing Environment using Quantum Key Distribution"**

Nowadays, Information Technology group is undergone significant shift in computing and protecting business value by using well-built, workable and authentic replacement of Cloud Computing. Cloud Computing is a contemporary computational architecture that provides another type of model. This paper proposes as a service of Advanced Quantum Cryptography in Cloud Computing. This paper discusses the security issues of cloud computing and the role of cryptography technique in Cloud computing to enrich the Information Security.

RONGZHI WANG et al. **"Research on Data Security Technology Based on Cloud Storage"**

Encryption storage, integrity verification, access control and verification and so on. through the data segmentation and refinement rules algorithm to optimize the access control strategy, using the data label verification cloud data integrity, using replica strategy to ensure the data availability, the height of authentication to strengthen security, attribute encryption method using signcryption technology to improve the algorithm efficiency, the use of time encryption and dht network to ensure that the cipher text and key to delete the data, so as to establish a security scheme for cloud storage has the characteristics of privacy protection.[1]

III. PROBLEM STATEMENT

Cloud computing is a basic technology for sharing of resources on the internet. Virtualization is a central innovation for empowering cloud resource sharing. Confidentiality of data storage is the essential alarm for assurance of data security so cloud computing does not provide robust data privacy. All details of data migration to cloud remain hidden from the customers. The problem in cloud computing environments are security of cloud computing. In this exploration we tended to the difficulties in fulfilling of cloud computing environment regarding security hazard implementation strategies on cloud computing environment and comparison of different cloud computing architecture through comparative study.

- In Existing system, there are following associate problems which are worked on our proposed work :
- AES-256 is quite common and easily available for hacker activity in case it desire to break.
- Existing accessing and storage scheme is slow in terms of computation time and process.
- Thus it exhibit high cost while storage of data, providing its availability to access.
- The existing algorithm use model which is still extension is required for proper loose coupling.
- Previous approach having limitation of accessing data from large structure of dataset.
- Highly indexed data structure is not taken in the base paper, which further need analysis of high end access.

IV. PROPOSED WORK

- The proposed work can be done in accordance of working with security and storage over the various available components.
- A product information outsourcing and searching system model including the data owner, cloud server and data users is designed.
- Two index structures supporting efficient product retrieval are constructed.
- The cloud storage audit protocol with secure outsourcing of key updates consists of eight algorithms (Setup, EiUpdate, ViESK, DiESK, AuthiGen, Proof - information, Proof - Verify and Check Proxy TPA).

4.1. Key Generation By Sha-2

SHA-2 contains the key length of 256 pieces, which is not flawed by the animal power assault framework, which is the main purpose of the hashing plan, as well as the security of the MAC if encryption should occur, where the highest number of security changes. Our proposed work means a high-security blend approach to cloud security management Hashes are convenient for situations where computers may want to identify, compare, or otherwise run calculations against files and strings of data. It is easier for the computer to first compute a hash and then compare the values than it would be to compare the original files.

Pseudo code for the SHA-256 algorithm follows. Note the great increase in mixing between bits of the w[16…64] words compared to SHA-1.

1. All variables are 32 bit unsigned integers and addition is calculated modulo 232
2. For each round, there is one round constant k[i] and one entry in the message schedule array w[i], $0 \leq i \leq 63$
3. The compression function uses 8 working variables, a through h
4. Big-endian convention is used when expressing the constants in this pseudocode,

When parsing message block data from bytes to words, for example, the first word of the input message "ABC" after padding is 0x41424380

Initialize hash values:

- First 32 bits of the fractional parts of the square roots of the first 8 primes 2..19

Initialize array of round constants:

- First 32 bits of the fractional parts of the cube roots of the first 64 primes 2…….311.

Pre-processing (Padding):

Begin with the original message of length L bits

- Append a single '1' bit
- Append K '0' bits, where K is the minimum number >= 0 such that L + 1 + K + 64 is a multiple of 512
- Append L as a 64-bit big-endian integer, making the total post-processed length a multiple of 512 bits

Process the message in successive 512-bit chunks: break message into 512-bit chunks for each chunk create a 64-entry message schedule array w[0..63] of 32-bit words

- The initial values in w[0..63] don't matter, so many implementations zero them here
- Copy chunk into first 16 words w[0..15] of the message schedule array
- Extend the first 16 words into the remaining 48 words w[16..63] of the message schedule array:
  for i from 16 to 63
    - s0 := (w[i-15] rightrotate 7) xor (w[i-15] rightrotate 18) xor (w[i-15] rightshift 3)
    - s1 := (w[i-2] rightrotate 17) xor (w[i-2] rightrotate 19) xor (w[i-2] rightshift 10)
    - w[i] := w[i-16] + s0 + w[i-7] + s1

Initialize working variables to current hash value:

a := h0 b := h1 c := h2 d := h3
e := h4 f := h5 g := h6 h := h7

Compression function main loop:

for i from 0 to 63
S1 := (e rightrotate 6) xor (e rightrotate 11) xor (e rightrotate 25) ch := (e and f) xor ((not e) and g)
temp1 := h + S1 + ch + k[i] + w[i]
S0 := (a rightrotate 2) xor (a rightrotate 13) xor (a rightrotate 22)
maj := (a and b) xor (a and c) xor (b and c)
temp2 := S0 + maj
h := g
g := f
f := e
e := d + temp1
d := c
c := b
b := a
a := temp1 + temp2

Add the compressed chunk to the current hash value:

h0 := h0 + a
h1 := h1 + b
h2 := h2 + c
h3 := h3 + d
h4 := h4 + e
h5 := h5 + f
h6 := h6 + g
h7 := h7 + h

Produce the final hash value (big-endian):
digest := hash := h0 append h1 append h2 append h3 append h4 append h5 append h6 append h7

Blowfish Algorithm For Data Encryption

The aboriginal footfall in the algorithm is to breach the aboriginal key into a set of sub keys. Specifically, a key of no added than 448 $.25 is afar into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit sub keys, while anniversary S-box contains 256 entries.This algorithm is disconnected into two parts.

1. .Key-expansion
2. Data Encryption

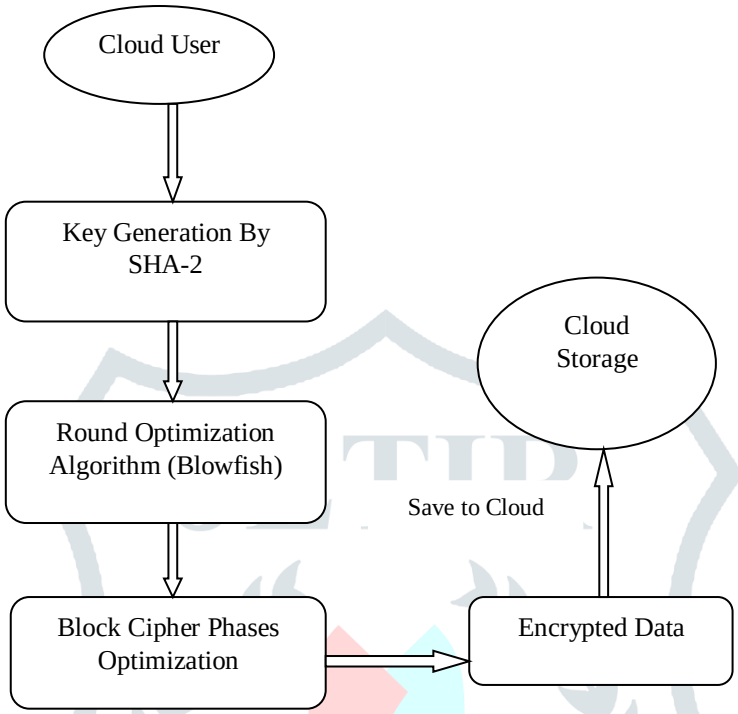

Figure: 3.4 Working Architecture of algorithms for encryption

4.2. Optimization Blowfish Algorithm

Our proposed strategy is working same as Blowfish calculation working , yet there is few point we have changed get the best outcomes.

A. Encryption Key size expanded
B. Reduce the Block (Phases)

The only change is S-boxes in the F-function. The Feistel structure of Blowfish algorithm is not changed but the structure of F-function is modified. The original Blowfish algorithm F-function has four S-boxes but the optimized Blowfish F-function has two S-boxes.

4.3. Pseudo-Code of Algorithm

A. Pseudo-code of F-Function with four S-Boxes (S0, S1, S2 and S3)

Step 1: Divide xL into four eight-bit quarters: a, b, c, and d
Step2: F(xL)=((S0,a+S1,b mod232)^S2,c)+S3,d mod 232

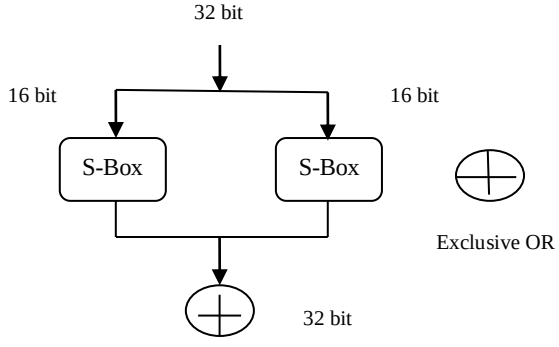

Figure 2: S-boxes break in Two Parts

B. The Pseudo-code of optimized F function with two S-boxes

Step 1: Divide xL into two sixteen-bit quarters: a, and b.
Step 2: F(xR)=(S0,a^ S1,b)

C. Pseudo-code of Encryption

Step 1: Divide the 64 bit input data into two 32-bit halves (left and right): xL and xR
Step 2: for i=0 to16 xL XORed with P[i]. Find F(xL) F(xL) is XORed with xR. Interchange xL and xR.
Step 3: Interchange xL and xR.
Step 4 : xR is XORed with P[16].
Step 5: xL is XORed with P[17].
Step 6: Finally combine xL and xR.

V. RESULT ANALYSIS

5.1.Encryption Time (Second) by used our approach the encryption time is reduced

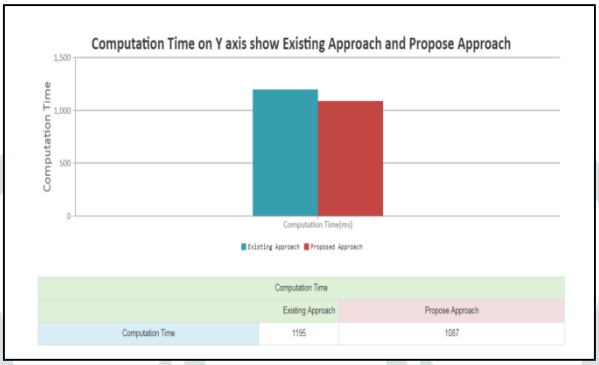

Figure 3: Encryption Vs Time

5.2.Throughput by used our approach the overall system Throughput increase.

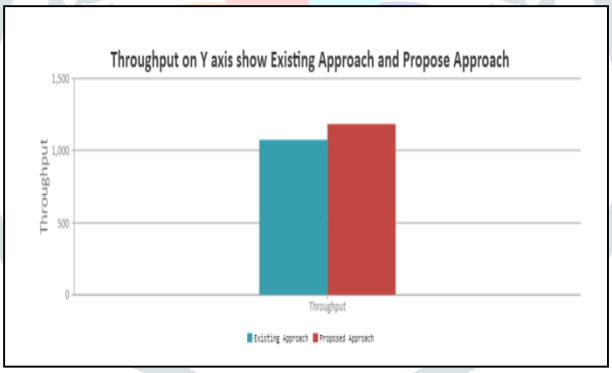

Figure 4: Throughput Vs Time

5.3.Decryption Time by used our approach the overall system Decryption time decrease

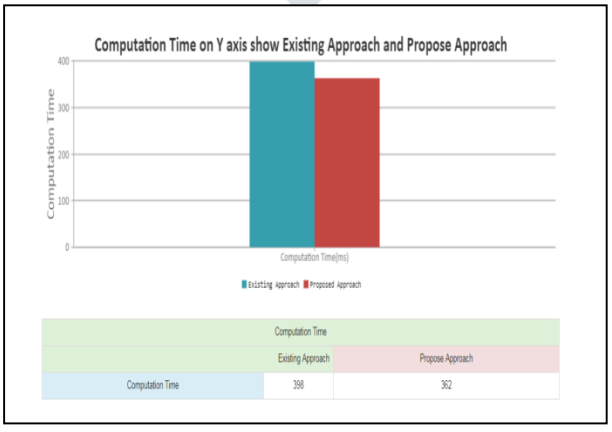

Figure 5: Decryption Vs Time

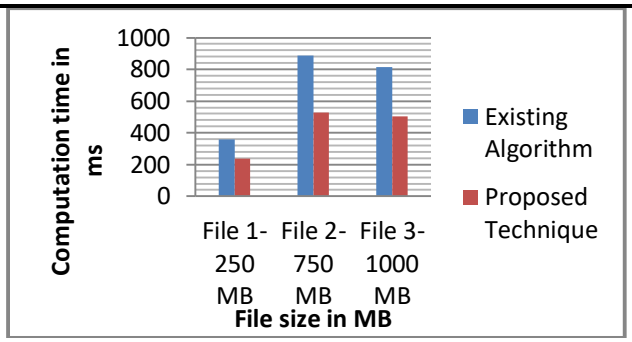

Figure 6: Computation Time Vs File Size

A Comparison analysis of the result obtained from the existing technique is made with our Technique. Our technique obtained better minimizing computing time while comparing with the existing compressive sensing, accessing approach. A Computation cost and other major analysis shows the efficiency of our technique

VI. Conclusion

Cloud computing by itself is in evolving stag security implications in it are not complete. It is evident that even the leading cloud providers such as Amazon, Google etc are facing many security challenges and are yet to stabilize. Achieving complete solution for are facing many security challenge With this level of issues in cloud computing decisions to adopt cloud computing in an organization could be made only based on the benefits to risk ratio. By checking a proxy server we will find out the fault in encryption. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the client end and the cloud server end. Main goal of cloud computing is securely store and transmit the data in cloud. As per analysis the proposed work compute the low time at TPA side as well as server side to process the data store at server side as well as manage and proof generation.

References

[1] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. ESpafford, “Secure outsourcing of scientific computations,” Trends in Software Engineering, vol. 54, pp. 215-272

[2] Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2010.

[3] Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An access control model for cloud computing", Elsevier journal of information security and applications, 2014.

[4] C. Wang, Q. Wang, K. Ren, N. Cao, W. LouToward secure and dependable storage services in cloud computing IEEE Trans. Services Comput., 5 (2) (2012), pp. 220-232

[5] Duncan, Adrian, Sadie Creese, and Michael Goldsmith . “Insider attacks in cloud computing.” Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE,201

[6] Pearson S. and A. Benameur: Security and trust issues arising from cloud computing. IEEE Second International Conference on Cloud Computing Technology and Science, CloudCom, pp. 693-702, 2010

[7] [10].M. M. Hassan, K. Lin, X. Yue, and J. Wan, “A multimedia healthcare data sharing approach throughcloud-based body area network,” Future Generation Computer Systems, vol. 66, pp. 48–58, 2017

[8] M. S. Hossain and G. Muhammad, “Healthcare big data voice pathology assessment framework,” IEEE Access, vol. 4, pp. 7806–7815, 2016.

[9] P. G. J. Leelipushpam and J. Sharmila, “Live vm migration techniques in cloud environment : A survey,” in Information Communication Technologies (ICT), 2013 IEEE Conference on, April 2013, pp. 408– 413.

[10] U. Varshney, Pervasive Computing and Healthcare. Boston, MA: Springer US, 2009, pp. 39–62

[11] A. Khan, M. Othman, S. Madani, and S. Khan, “A survey of mobile cloud computing application models,”ommunications Surveys Tutorials, IEEE, vol. 16, no. 1, pp. 393–413, First 2014.

[12] Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou, “A Hybrid Cloud Approach for Secure Authorized Deduplication”, IEEE Transactions on Parallel and Distributed Systems, 2014.

[13] Po-Wen Chi ; Chin-Laung Lei” Audit-Free Cloud Storage via Deniable Attribute-Based EncryptionSign In or Purchase” IEEE Transactions on Cloud Computing (Volume: 6, Issue: 2, April-June 1 2018)

[14] Luo Yuchuan ; Fu Shaojing ; Xu Ming ; Wang Dongsheng” Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage Sign In or Purchase” China Communications (Volume: 11, Issue: 11,Nov 2014)