International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Optimized Storage and Secured Data Transaction in Cloud Environment using ECC and Huffman Encoding

Saket Nigam[1], Rekhansh Rao[2]

[1]Computer Science and Engineering, Rungta College of Engineering and Technology, Bhilai, India

[2]Professor, Computer Science and Engineering, Rungta College of Engineering and Technology, Bhilai, India

Abstract: ***Cloud Computing services addresses the problems of privacy and security. For providing such services, it takes the help of internet. It helps users in accessing files and using applications. These services can be used according to user's demand and usage requirements. It helps in storing data from more than one client. It grants remote access of data to users. It saves cost and there is no need for buying storage devices. It also helps in preventing loss of information system failure. Cloud computing is a computing structure in which computer infrastructure resources are provided as service to users. This is done through the help of internet. This technology helps in accessing their files and application remotely. It can be done through any other computer. Cloud based services include software, platform & infrastructure as services. These services allows users to take benefits of such services where as demand arises. These services are usage based and are purchased on the basis of need & timely requirements. These area unit several benefits of cloud storage of information, however the most problems area unit associated with security & access management as a results information |of information} storage on severs don't seem to be at intervals constant positive domain as knowledge householders. For the purpose of security & maintenance of confidentiality, cryptography is used .all this is done from the help of internet. Cloud storage provides a platform for applications and infrastructure related services. Most of the information, which is store in cloud is sensitive.***

Keywords: Access control, Authentication, Attribute-based signature, Attribute-based encription, cloud storage, cast minimizing

1. Introduction

Cloud Security: At a moment, hundreds of users can access the cloud storage. Hence, cloud security is a major concern. With the help of the KDC, we store data in cloud. Management of the cloud user‛s identities are done through common mechanisms such as-Authentication, Authorization, Account management, Audit logging. Authorization is a process which helps in deciding the limit allowed for the user to access & is generally handled by the application being accessed. Authorization is granted purely on the basis of user identity. Many applications generally use centralizing policy decision to authorize access to user & not considering the location of application. It is of utmost importance to preserve users privacy & helping in maintaining user anonymity also. Users can access & modify/alter resources. Raw data is data which has been processed. The main difference between data & information is that information is the end result of data processing, is known as cooked data.

Cryptography is a type of method which helps in storage & transmission of data safely and securely. It transforms and transmits the data in such a form that it may only be read by the person to whom the information was intended to be sent. It is very important to address the issue of identity anonymity & secured data storage in cloud.

Cipher text it is also known as encrypted text. In the terms of cryptography, cipher is an algorithm Which helps in conversion of plain text into cipher text. Cipher text is also known as encrypted/encoded information because it is not possible to read by human or computer without the proper algorithm. The opposite of encryption in decryption. It is the process of converting cipher text book into plain/clear text. Code text &cipher text are altogether different. Code text is a result of code, not a cipher.

2. Group Signature

Digital signatures are extensively used for offering services like data integrity, entity authentication, data origin authentication etc. An anonymous digital signature is a special type of signature in which any entity, even the verifier , can not find out signer‛s information. Group signature permits cluster, a gaggle, a bunch} members to check in behalf of the cluster member to sigh on behalf of the group anonymously. The signatures can be verified using a single group public key. Differentiation between two group signature is not possible. In case of dispute , only the group manager has the power to disclose the identity of group member. Group signatures are publically verifiable & can be verified with respect to a single group public key.

2.1 Properties of Group Signature:

A secure group signature scheme satisfies the following properties:

- **Anonymity:** For a particular signature, identification of real signer is not possible except for the group manager.
- **Unlink ability:** Deciding whether 2 different signature is made by the same signer is very hard.
- **Enforceability:** Only member are authorized to sign messages on behalf the group.
- **Correctness:** Signature produced by a group member must be provable.
- **No framing:** The group members or the group manager can not sign messages for the other members.

- **Traceability:** The group manager can be always relied upon to prove the validity of the identity of a member.
- **Excludability:** Even if the group manager or some of the group members join together, they can not sign on behalf of other group members.

Identity Based Cryptography: Due to Shamir the concept of identity based cryptography is introduced. A publically known identifier for address for example , email address, IP address is introduced by this system and the name to be used as the public key component of a public/private key pair in cryptography system is an identity based cryptography system. The assumption of scheme is that they believe on the presence of trusted authority whose only purpose is to compute for each user the private key associated with the identifier they wanted to use as public key. This scheme is ideal for closed group of the users. various identity (ID) based schemes have been proposed. And some of these elliptic curve (EC) algorithms so that particularly efficient.

The basic characteristics of identity base cryptosystems are used by the identity based group signature scheme. In this system encryption of plaintexts or verification of signatures does not need to be referred to a certificate authority, for public keys. in the case of group signature the verification of output ―opening”. Or verification of the group signature or both can be considered as identity.

Amazon‟s EC2 was the first one who started the commercialization of cloud computing in 2006. In a very famous in all over the world. Because cloud has faster technology growth, US govt. wants to apply the cloud computing platform in apply the cloud computing platform in their federal infrastructure over the period 2013-2018, and it has taken huge steps for implementation . it is predetermined that the annual federal cloud computing market will achieve landmark of $10 billion by 2018. The US federal govt‟s cloud computing market will achieve a 16 % compound annual growth rate over the period.

3. Literary Survey

Cloud can be used for strong business and personal data by user. Therefore CDS‟S are responsible for providing since the commercialization, low cost services have proved themselves as great challenges to service providers. Very few researchers have thought about cloud storage and its cost minimization by the help of data storage space minimization. Most researchers suggested that costs can be minimized by reducing power consumption and maximizing resource utilization. Three procedures have been identified to improve data centre efficiency and cost minimization.

1) Increased datacenter network agility.
2) Pursuing design algorithm and market mechanism for optimization of resources.
3) Geo-divecified data centre for improvement in performance and negligibility.

Privacy protective Access management With Authentication for Securing knowledge in Clouds: Sushmita Ruj, Milos Stojmenovic and Amiya Nayak proposed a scheme, An user can create a file and store it securely in the cloud by using attribute based encryption and attribute based signature and define working method. in this scheme prevents replay attacks and supports creation, modification and reading data store in cloud. This scheme provide fine-grained access control and authenticates users who store information in the cloud. This scheme support one use can write while many users can read. It is robust and decentralized. computational load of user during read, minimum comparable cast as compare to centralized approaches [1] is totally fixed (i.e. 'a' is usually specifically 97). In apply, it's not the case that every one 256 characters within the ASCII set occur with equal frequency. In AN English text document, it'd be the case that solely ninety roughly distinct characters square measure used the least bit (meaning 166 characters within the ASCII ne'er even appear) and at intervals those ninety there square measure doubtless to be vital variations within the character counts.

Huffman is AN example of a variable-length encoding— some characters might solely need a pair of or three bits and different characters might need seven, 10, or 12 bits. The savings from not having to use a full eight bits for the foremost common. The classical RSA algorithmic rule used for authentication is used in some parameter .

ASCII Encoding

The example we‟re about to use throughout this handout is coding the actual string "happy hip hop" (don‟t question me what it suggests that, I simply created it up!). exploitation the quality code coding, this 13- character string needs 13*8 = 104 bits total. The table below shows the relevant set of the standard code table.

Char	code	bit pattern (binary)
h	104	01101000
a	97	01100001
p	112	01110000
y	121	01111001
i	105	01101001
o	111	01101111
area	32	00100000

The string "happy hip hop" would be encoded in code as 104 ninety seven 112 112 121 thirty two 104 one zero five 112 thirty two 104 111 112.

Although not simply decipherable by humans, it might be written because the following stream of bits (each computer memory unit is boxed to point out the boundaries):

01101000 01100001 01110000 01110000 01111001
00100000 01101000 01101001 01110000 00100000
01101000 01101111 01110000

To decipher such a string (i.e. translate the binary coding back to the first characters), we have a tendency to just have to be compelled to break the encoded stream of bits up into 8-bit bytes, then convert every computer memory unit exploitation the mounted code coding. the primary eight bits ar 01101000, that is that the pattern for variety 104, and position 104 within the code set is assigned to minuscular 'h'. A file encoded in code doesn't need any extra info to be decoded since the mapping from binary to characters is that the same for all files and computers.

4. Problem Identification

All these approaches became centralized approach and allow only KDC. In all these cases, decryption at user‗s end is computation intensive. That is why if a user is using their mobile devices/handled these technique might be ineffective from assessment.

5. Solution of the Problem

In this theme the presence of 1 proxy and one KDC makes it less forceful than decentralised approaches along these approaches had no thanks to validate users, anonymously. to supply safe and quick access to cloud for a licensed user while not revealing his identity however the user needs the opposite user to understand that he's a legitimate user. the problems of access management, authentication, and privacy protection unit of measurement resolved.

6. Proposed Methodology

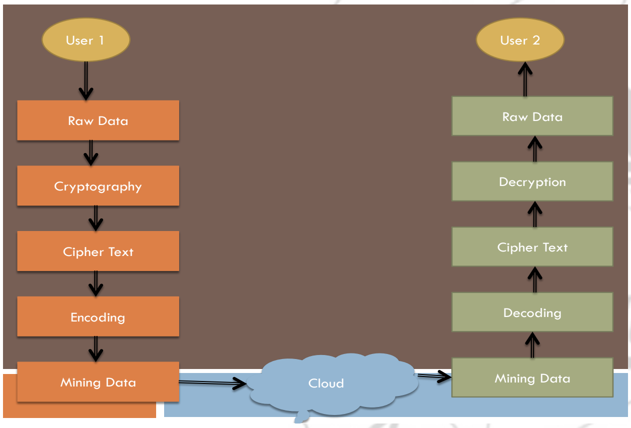

Figure 1: Proposed System Architecture

Privacy protective access management with authentication theme planned within the paper may well be improved or altered for the improvement of cloud security system with the effective storage.

Example:
Algorithm based encryption system can be alter with electivity curve based encryption system. Simple rationalization for Elliptic Curve science rule the equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,
E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)

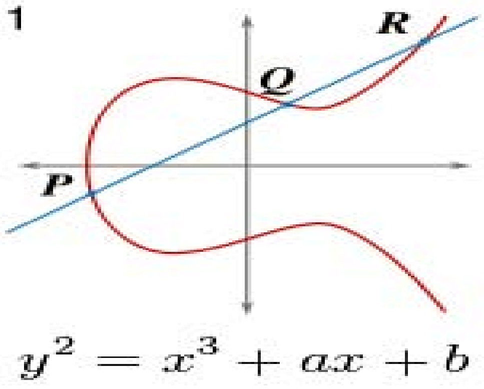

Figure 2: Elliptic Curve

Key Generation
Key generation is a crucial half wherever we've got to get each public key and personal key. The sender are encrypting the message with receiver‗s public key and therefore the receiver can rewrite its non-public key.
Now, we've got to pick variety ‗d‗ among the vary of ‗n‗.
Using the subsequent equation we are able to generate the general public key
Q = d * P d = The random range that we've got chosen among the vary of (one to n-1). P is that the purpose on the curve.
‗Q‗ is that the public key and ‗d‗ is that the non-public key.

Encryption:
Let ‗m‗ be the message that we tend to area unit causing. we've got to represent this message on the curve. This have in-depth implementation details. Consider ‗m‗ has the purpose ‗M‗ on the curve ‗E‗. arbitrarily choose ‗k‗ from [1 – (n-1)].
Two cipher texts are generated let it's C1 and C2.

C1 = k*P
C2 = M + k*Q
C1 and C2 are send.

Decryption:
We have to urge back the message ‗m‗ that was send to us,
M = C2 – d * C1
M is that the original message that we've send

Proof:
How will we tend to come back to the message,
M = C2 – d * C1
‗M‗ will be pictured as ‗C2 – d * C1‗
C2 – d * C1 = (M + k * Q) – d * (k * P)
(as a result of C2 = M + k * Q and C1 = k * P)
= M + k * d * P – d * k *P
(cancelling out k * d * P)
= M (Original Message)

A variable-length encoding
What if we tend to drop the necessity that each one characters take up constant variety of bits? By exploitation fewer bits to encrypt characters like 'p', 'h', and house that occur of times and additional to encrypt characters like 'y' and 'o' that occur less of times, we tend to could also be ready to compress even additional. We‗ll later show however we tend to generated the table below, except for

currently simply take our word for it that's represents associate optimum Huffman encryption for the string "happy hip hop":

Char bit pattern

h	01
a	000
p	10
y	1111
I	001
o	1110
space	110

Each character incorporates a distinctive bit pattern secret writing, however not all characters use a similar variety of bits. The string "happy hip hop" encoded victimisation the on top of variable-length code table is:
01 000 10 10 1111 110 01 001 10 110 01 1110 10

The encoded phrase needs a complete of thirty four bits, shaving some a lot of bits from the fixed-length version. what's tough a few variable-length code is that we have a tendency to now not will simply confirm the boundaries between characters within the encoded stream of bits once decryption. I boxed each different character's bit pattern on top of to assist you visualize the secret writing, however while not this aid, you may surprise however you may grasp whether or not the primary character is encoded with the 2 bits 01 or the 3 bits 010 or maybe simply the primary bit 0? If you explore the secret writing within the table on top of, you may see that only 1 of those

Encoding seen as a tree
One way to examine any explicit encryption is to diagram it as a binary tree. every character is hold on at a leaf node. Any explicit character encryption is obtained by tracing the trail from the basis to its node. every left-going edge represents a zero, every right-going edge a one.

Encoding the File Traverse Tree for Codes
Perform a traversal of the tree to obtain new code words
Going left is a 0 going right is a 1 code word is only completed when a leaf node is reached

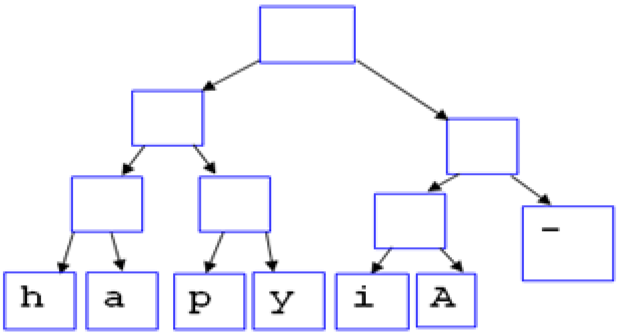

Figure 3: Encoded Tree

7. Results

Enhancement of cloud security system is expected to be the main outcome from the study. more reliability and security can be based on curve based encryption system with the help of half-man technique. This technique can be used in the implementation in cloud with respect to security and minimization of cost . If a member in a group wants access of a file without the provider of cloud service knowing about it, the participation of trusted third party user is required. The identity of sender will obviously be exposed if the request is sent directly to cloud service provider. Even an anonymous request will not be able to convince the service provider that the person is authorized to access the details. In realistic terms, the group manager should be able to trace the identity of the signer. The group has to provide guarantee to the receiver that the signature produce was legitimate. In case of dispute the group manager must be able to reveal the identity of the signer.

Comparison of our scheme with existing access control schemes

Schemes	Fine-grained access control	Centralized/ Decentralized	Write/read Access	Type of access control	Privacy preserving Authentication
29	yes	Centralized	1-W-M-R	Symmetric key cryptography	No authentication
10	yes	Centralized	1-W-M-R	ABE	No authentication
11	yes	Centralized	1-W-M-R	ABE	No authentication
14	yes	Decentralized	1-W-M-R	ABE	No authentication
13	yes	Centralized	M-W-M-R	ABE	Authentication
ours	yes	Decentralized	M-W-M-R	ABE	No Authentication

We have performed experiments to evaluate the performance in cloud environment. When we compare to our scream with RSA (Rivest-Shamir-Adleman) Algorithm than entropy value higher with respect to data length size.

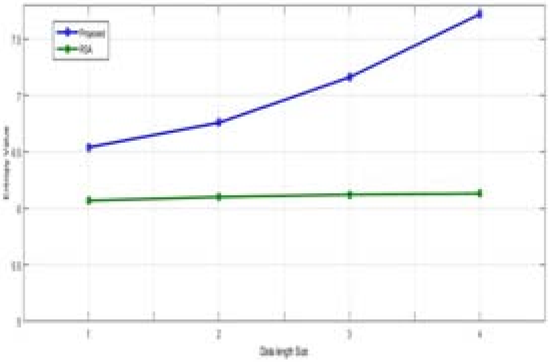

Figure 4: Entropy value and Data Length

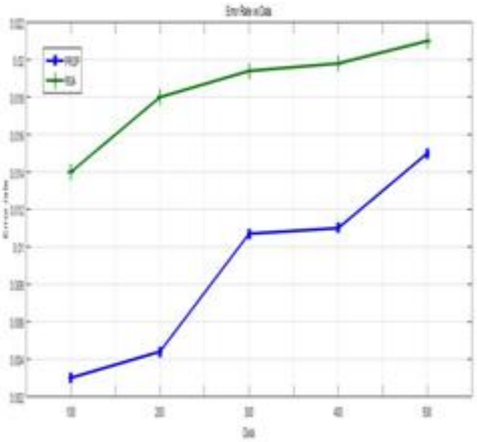

Figure 5: Various Phases of Outcome

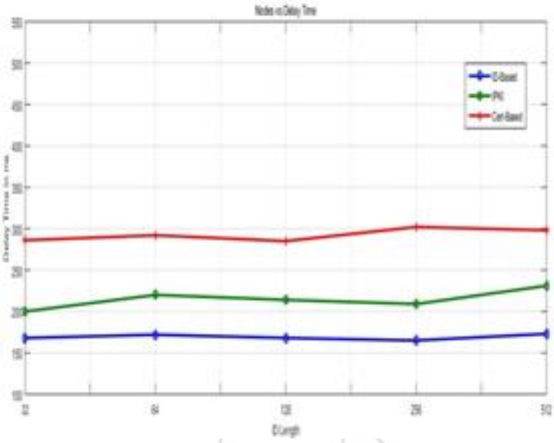

Figure 6: Node Vs Delay Time

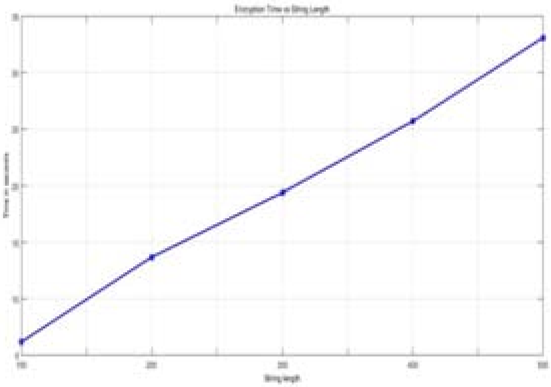

Figure 7: Encryption Time VS String Length

8. Conclusion

Identity based cryptosystem is useful in creation of anonymous signature for authorization of user from a group .the provider of cloud service will not know the individual identity of user. He will know when a group which has been authorized will access the cloud .the number of members in a group does not define the size of the key and the length of signature involved. The scheme of identity based cryptosystem has the following properties –

1) Authenticity
2) Signer anonymity
3) Traceability of signer

This system helps applications where group identities are involved like e-auction, e-voting etc. creative approaches have been designed for automatic login and access of data in cloud. These approaches also involve mechanism of auditing. the approach we have proposed makes it possible for user for not only auditing of his data and its contents but also provide back-end protection when required.

References

[1] S. Ruj, M. Stojmenovic and A. Nayak, ―Privacy Preserving Access Control with Authentication for Securing Data in Clouds", *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 556–563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, ―Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T. Services Computing*, vol. 5, no. 2, pp. 220–232, 2012

[3] H. Li, Y. Dai, L. Tian, and H. Yang, ―Identity-based authentication for cloud computing," in *Cloud Com*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, 2009, pp. 157–166.

[4] A.-R. Sadeghi, T. Schneider, and M. Winandy, ―Token-based cloud computing," in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer, 2010, pp. 417–429.

[5] G. Wroblewski, ―General method of program code obfuscation," Ph.D. dissertation, Wroclaw University of Technology, 2002. http://www.ouah.org/wobfuscation.pdf.

[6] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, ―Trustcloud: A framework for accountability and trust in cloud computing," HP Technical Report HPL-2011-38. Available at

[7] http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[8] D. F. Ferraiolo and D. R. Kuhn, ―Role-based access controls," in *15th National Computer Security Conference*, 1992.

[9] D. R. Kuhn, E. J. Coyne, and T. R. Weil, ―Adding attributes to role-based access control," *IEEE Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[10] M. Li, S. Yu, K. Ren, and W. Lou, ―Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *SecureComm*, 2010, pp. 89–106.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, ―Attribute based data sharing with attribute revocation," in *ACM ASIACCS*, 2010, pp. 261–270.

[12] G. Wang, Q. Liu, and J. Wu, ―Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *ACM CCS*, 2010, pp. 735–737.

[13] F. Zhao, T. Nishide, and K. Sakurai, ―Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, vol. 6672. Springer, 2011, pp. 83–97.

[14] S. L. Garfinkel, "Technical report tr-08-07: An evaluation of amazon's grid computing services: Ec2,

s3 and sqs." Computer Science Group, Harvard University, Cambridge, Massachusetts, Tech. Rep 2007.

[15] Market research media. 2013. U.S. Federal Cloud Computing Market Forecast 2013-2018. [Online] Available: http://www.marketresearchmedia.com/?p=145. [Accessed 04 October 2013].

[16] S. Rivoire, M. A. Shah, P. Ranganathan and C. Kozyrakis, "JouleSort: a balanced energy-efficiency benchmark." *Proceedings of the 2007 ACM SIGMOD international conference on Management of data. ACM, 2007.*

[17] A. Greenberg, J. Hamilton, D. A. Maltz and P. Patel, "The cost of a cloud: research problems in data center networks." *ACM SIGCOMM Computer Communication Review 39.1 pp. 68-73, 2008.*

[18] A.H. Mohsenian-Rad, and A. Leon-Garcia, "Energy-information transmission tradeoff in green cloud computing." *Carbon 100 (2010): 2011(2010): 200.*

[19] J. Baliga, R. W. A. Ayra, K. Hinton and T. RodneyS "Green cloud computing: Balancing energy in processing, storage, and transport.—*Proceedings of the IEEE 99.1 pp. 149-167, 2011*