Key Generation using Ternary Tree based Group Key Generation for Data Encryption and Classification

Nikita Gupta
M.E.(CSE) Scholar
Department of CSE
Truba Institute of Engineering & Information Technology,
Bhopal, India

Amit Saxena
Associate Prof. &Head
Department of CSE
Truba Institute of Engineering & Information Technology,
Bhopal, India

ABSTRACT
Here in this paper a new and efficient technique for the Cohort of Keys using Tree based Algorithm is proposed for the Sharing of Data in Secure manner. The Key Group Procedure is implemented for the Sharing of Data where Data Owner who needs to send Data is first Encrypted Information using Tree grounded Key Group and then when Data is received at the other end it is decrypted and Classify as Normal or Abnormal Packet. The Planned Practise realized provides Privacy from various attacks as well as provides less computational and Communication Cost.

Keywords
Tree based Key Generation, AES, User Revocation, Entropy, Network Security, Group Key Establishment.

1. INTRODUCTION
As data in Cloud is dynamic, static auditing is not an adequate amount of cloud environment. A dynamic auditing is required to authenticate the data integrity of the dynamic data. But as data are self-motivated in cloud, it is not uncomplicated to have an auditing competently. Server can put into effect replay attack and counterfeit attack to fail the auditing procedure. The dynamic procedures consist of alteration, insertion and deletion. Whenever you like dynamic operation is achieved the owner sends to bring up to date message to the auditor characterizing the index number of that message. The auditor updates the table. The message m and the tag are reinstated by the new message and tag in message modification. The new message m and new tag are inserted in insertion operation. The message m and tag are deleted from the index table and all the entries below the deleted message move upwards. After performing updates in the table, the auditor conducts the data integrity test for the keep informed data. Auditor sends the consequence to the owner and he deletes the local copy of keep informed data.

As the quantity of cloud provider's enlarges, deciding a trusted service became deadly. The auditing method is essential to make your mind up the cloud integrity concerns. There are dissimilar checking assembly recommended in cloud calculating. But most of them are motionless in situation and they are put into experienced by cloud earners.

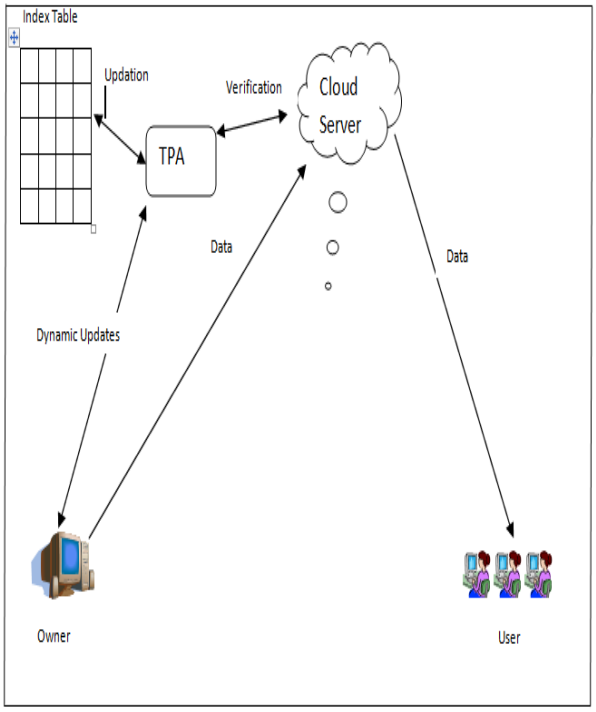

Fig 1: Dynamic TPA System

With the purpose of have active investigative, Active Third Party Auditing System is recommend. The welfares of cloud computing are strong, so is the need to mature correct security for cloud implementations. In totaling to the typical contests of emergent secure IT organizations, cloud calculating offerings an additional level of risk since indispensable amenities are often outsourced to a third party. The expressed feature of subcontracting makes it solider to preserve data honesty and confidentiality, sustenance data and provision handiness, and validate acquiescence. For well group it is very indispensable that cloud that permits examination from a solitary party. Audit the outsource information to guarantee the data refuge and save the user's addition and information stowage. It is very significant to deliver public reviewing service for cloud data storage, so that the user trusts an sovereign third gathering auditor (TPA). TPA draughts the honesty of information on the cloud on the behalf of the workers, and it delivers the rational way for the workers to checkered the rationality of information in the cloud. On the whole, permitting community reviewing amenities plays a energetic role in starting cloud budget, where by workers need way to evaluate to jeopardy and gain confidence in the mist [1].

Public reviewing in calculation to user delivers the outside party to authenticate the exactness of deposited statistics against the outdoor occurrences. However these schemes [2], [3], [4] don‘t contain the confidentiality fortification of the information. It is a main drawback which touch the refuge of the procedures in cloud calculating.

1.1 Third Gathering Auditor

The third festivity auditor (TPA), who has proficiency and competences that fog users do not have and is important to evaluate the cloud stowage provision refuge on behalf of the user upon demand. Operators trust on the CS for mist information stowage and conservation. They may also vigorously cooperate with the CS to admittance and apprise their deposited information for several submission determinations [5]. The manipulators may alternative to TPA for guaranteeing the stowing sanctuary of their subcontracted statistics, while hopeful to keep their figures sequestered from TPA.

We deliberate the reality of a semi-trusted CS as does. Namely, in greatest of time it performs appropriately and does not diverge from the agreed etiquette implementation [6] [7]. Though, throughout on condition that the cloud information stowage grounded amenities, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users.

1.2 Group Key Establishment

In general, GKE protocols present multiple phases

1.2.1 Initialization

It defines the environment of the protocol: the parameters, the space of all possible keys and any other prerequisites.

1.2.2 Users Registration

It assigns group membership to users. Depending on the scenario, after registration, a user may for example share a secret key (or password) with a trusted group authority or may generate a certified long-lived public-private key pair for later signing purposes.

1.2.3 Execution

It describes the cryptographic algorithm, including the performed computations and the exchanged messages. It frequently entails of multiple rounds of communication between principals. from the knowledge he gained after the Execution Phase. It is sometimes integrated within a round of the execution phase.

1.2.4 Key Confirmation

It confirms that all the intended members actually own the key and no other except them does. Although it is an optional phase, it is usually performed for security reasons.

1.2.5 Key Computation

It explicit the key computation formulas or algorithms performed by a party to derive the key

1.3 Informal Security Requirements

A GKE protocol should satisfy a set of properties, which we informally recall next. Key confidentiality (also called key privacy, key secrecy or non-disclosure) [8], [9] guarantees that it is (computationally) infeasible for an adversary to calculate the collection key. The stronger notion of known key security assures that key confidentiality is maintained even if the attacker somehow manages to obtain group keys of previous sessions.

Backward secrecy [10] conserves the privacy of future keys regardless the adversary's actions in the past sessions. Congruently, advancing secrecy [10] executes that the challenger movements in forthcoming runs of the procedure do not negotiation the confidentiality of preceding assembly solutions (i.e. a key remnants protected in the forthcoming). Key selection must satisfy specific properties. Key freshness requires that the collection key has certainly not been used before. The related concept of key independence imposes that no correlation exists between keys from different sessions; this means that (cooperation between) authorized participants to distinct sessions of the protocol cannot disclose session keys they are unauthorized for. In addition, key randomness warrants key in-distinguish ability from a random number and hence key unpredictability. Two other important security requirements regarding the key value exist: key integrity which attests that no adversary can modify the group key and key consistency, which prevents different players to accept different keys.

Group member authentication represents a mandatory condition for group cryptographic protocols. Entity authentication confirms the identity of a participant to the protocol to the others. Similarly, unknown key share resilience restricts a user to trust that the important is shared with one party when in fact it is shared with another. Key negotiation impression (KCI) resilience [11] prevents an attacker who owns the long-lived key of a participant to impersonate other parties to him. The stronger property named ephemeral key leakage (EKL) resilience (EKL) [12] avoids an adversary to recover the group key even if he discloses the long-lived keys and ephemeral keys of parties involved except both these values for participants in the test session1. (Implicit) Key authentication limits the possible owners of the collection key to the genuine contributors; this means that no other party except the qualified users is capable to compute the key, but it does not necessary mean that all legitimate principals actually own it. Another property, called key confirmation certifies that all authorized members actually have the key; however, it does not claim that no other party owns the same key. Explicit key authentication (or Mutual Authentication (MA)) [13], [14] combines these notions and ensures that all qualified participants to the protocol have actually computed the group key and no one else except them have.

2. LITERATURE SURVEY

The Author planned a new agenda architecture for the Key Generation on Pairwise Independent Networks [15]. The two main components i.e. resident key cohort and comprehensive key dissemination is implemented. Local Key Generation is used for Point-to-point foundation coding with side material from which diagram can be raised and comprehensive key propagation is used to deliver various Secrete Keys. Complex Algorithm for key generation and hence take more computational time.

K. Kalaivani, K. Renugadevi, Nithya also planned a new outline for the Pairwise Sovereign System using Key Cohort Procedure [16]. Here an Efficient Two Secrete Key generation for low complexity using local key generation and global propagation is proposed which provides better performance. Complex Algorithm for key generation and hence take more computational time.

SirinNitinawarat, Chunxuan Ye, Alexander Barg planned a new and efficient technique for the Secrete Key Group for a Pairwise Autonomous System Model [17]. The unbiased is to

engender a undisclosed key collective by a given subcategory of terminuses at the principal rate probable, with the collaboration of any outstanding terminuses. A (single-letter) formula for clandestine important volume brings out a ordinary assembly amongst the problematic of underground key group and a combinatorial problematic of greatest stuffing of Steiner trees in an related multigraph. High Storage Cost and Inefficient key generation.

Peng Xu, Zhinguo Ding, Xuchu Dai implemented a private key capacity based Cooperative Pairwie Independent Network [18]. In this broadside associated foundations pragmatic by every pair of terminuses are self-determining of those foundations pragmatic by any other pair of mortal. All the termini can transfer with each other over a communal conduit which is also experimental by Eve quietly. The detached is to produce a isolated key amongst Alice and Bob under the help of the M communicates; such a isolated key desires to be dwindling not only from Eve but also from separate relays instantaneously. High storage capacity for secrete keys is required.

3. PROPOSED METHODOLOGY

Here the proposed code is grounded on the notion of entropy variation.

The proposed code implements for three types of data packets.

1. Normal Message data
2. Media file
3. KDDCUP 99 dataset

The flow of methodology starts with pre-shared authentication between sender and local router. The main aim of using the concept of pre-shared is the detection of un-authorized user at the local router so that no data is send to the server side. The key is shared between a number of users and local router and each time a user needs to send the data to the server it needs to be authenticated on the local router. If it is valid user the it can send data to the server through local router which includes message, media or dataset. The next phase of the codes contains detection of abnormal data send by the user using the concept of entropy variation. The data when send by the normal user the entropy is less whiles it increases for the abnormal data.

For the calculation of data contains which type of attack J48 classification tree is generated through which rules are generated and hence we can identify the type of attack.

3.1 Generation of Rules from the dataset

Here the rules are generated based on decision tree using J48.

```
*********************************************
                Rule-1
*********************************************
if (logged_in) equals '1' then
        packet flow is "Normal"

*********************************************
                Rule-2
*********************************************
if (logged_in) equals '0' then
        if (src_bytes) > '240' then
                packet contains "Smurf" Attack

*********************************************
                Rule-3
*********************************************
if (logged_in) equals '0' then
        if (src_bytes) <= '240' then
                if (dst_host_serror_rate) <= '0.5' then
                        Packet contains "nmap" attack
                else if (dst_host_serror_rate) > '0.5' then

                        Packet contains "neptune"  attack
```

The proposed procedure includes the following set of steps for the detection of interruptions in the dataset.

1. Initially set up a network with no. of sender of local routers between them and preshared key between them which needs to be exchanged for authentication.
2. For ‘N’ number of packets send from source ‘S’ to Destination ‘D’.
3. The local router ‘R’ checks the authenticity of the Source ‘S’.

Algorithm for Key Generation using Ternary Tree Based Group Key Generation

1. Let total no of node is **n.** so we divide them in a sub-group of 3-nodes.if total no of node is not multiple of 3 then remaining node form a group (it may contain 1 or 2 node).we given each group a unique integer as ID.

2. In each group we randomly choose any one node as GC (group controller).It further communicate to other GC to compute final Group Key.

Then each sub-group computes their Group Key as following: Let it G1(group 1, 1 is id).it contains 3 nodes, these are N11,N12,N13 .N11 choose a random no a1 and compute **a1P**.Then it sends it to N12. Now N12 choose another random integer a2 and computes **a1a2P** and **a2P**.Then it sends to N13.Now N13 calculates indicate arbitrary no a3 and subtracts **a3P**, **a2a3P** and **a1a2a3P**.It preserve **a1a2a3P** as clandestine Significant and other 2 conducts to the N11.Now N11computes **a1a3P** and **a1a2a3P**.sends **a1a3P** to N12 and it will figures **a1a2a3P**. After this each GC come forward for further computation. They again form a group of 3 member and compute shared key as previous. In this way when final key is computed then each final group member send this key to their sub-ordinate group member as message encrypted by their previous generated shared key. After receiving message each user decrypt it using their previous computed shared key. Common key computation with-in a sub-group (3 nodes).

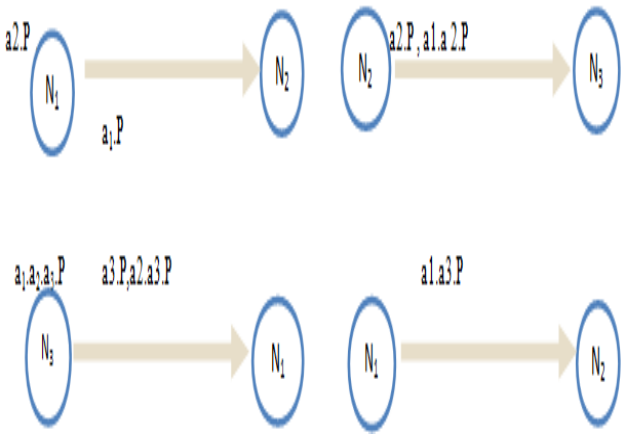

Fig 2. Common key computation with-in a sub-group

4. If Source is valid user then entropy of the communication can be subtracted by the other router 'R2'.

Algorithm for Entropy variation

a. If 'N' number of packets send from 'R' → 'R2.
b. Repeat for all packets 'pkt'
c. En=calculate_entropy('pkt')

Pseudo Code for Entropy Variation

```
Calculate_entropy('pkt")

for (int c_ = 0; c_ < s.length(); ++c_) {
    char cx = s.charAt(c_);
    if (occ.containsKey(cx)) {
      occ.put(cx, occ.get(cx) + 1);
    } else {
      occ.put(cx, 1);
    }
    ++n;
double p = (double) entry.getValue() / n;
    e += p * log2(p);
```

d. If En > threshold value
e. Alarm for the tracing of packet attacker is generated
f. Else
g. No alarm is generated
h. End

3. RESULT ANALYSIS

SECURITY ANALYSIS

Replay Attack

It is a type of bout in which the victim applies a random unique key again and again since the key breaks. But replay attack is prevented by the proposed methodology since token key gets destroys after a particular time stamp.

Man in the middle attack

This type of attack mainly occurs when a sender sends data to the receiver and during the transmission of message third party attacks in between and access data in an un-authorized manner.

Brute force attack

Brute force attack are the process of brute force search, in general apply all the possibilities of the key. In our planned arrangement there are no chance of this type of attack, because of key length is very large in our method, so it take lot of time to apply all possibilities. Second thing is that our key life time is very short so there are no chances of brute force attack.

Dictionary attack

A dictionary attack is another type of password guessing attack which uses a dictionary of common words to identify the user's password. In our proposed method we used master key as a password so there are no common word in this password that means there are no chance of the dictionary attack.

Confidentiality

Confidentiality means that when a sender want to send a message or data to the receiver then the message can be read by only that particular receiver not by the other .For Example one party may to show his key to the other party and the other one may try to attack the other party then this time using OTPK, the session is for a limiting time and the generating of master key is randomly and it gets destroyed each time.

Authentication

Authentication means receiver must be insure that the message can not be alter or edit after sending by the sender. This property is making sure that the signature verification must be done by both the parties also by the TTP. When we perform contract signing between two parties then the authentication is very important.

Table 1. Other additional security analysis

Security Parameter	Prevented by proposed technique
Insider attack	YES
Password impersonation	YES
Password guessing attack	YES
Outsider attack	YES
Denning sacho attack	YES
Public verifiability	YES

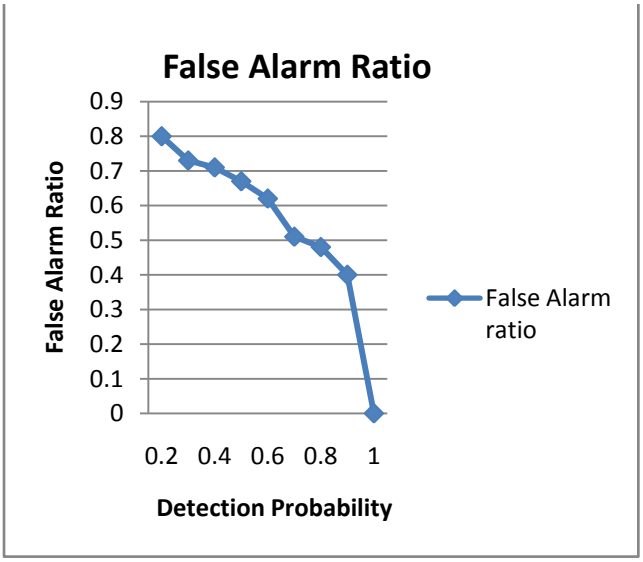

Fig 3. Analysis of False Alarm Ratio

Table 3 shows, the storage judgment of the planned scheme with the relevant user authentication based on smart card, which shows our proposed scheme is reduced burden on the server, because the Server has stored less storage.

Table 3: storage judgment of the planned scheme

Storage/ scheme	Our scheme
Data Owner	520 bits
Receiver	64 bits

The Table shown below is the analysis and comparison of number of keys generated at the encryption and decryption on the basis of number of users available in the group.

Table 4. Analysis of Number of Keys Generated

	No. of Keys Generated	
No. of Groups	**Existing Work**	**Proposed Work**
1	(1,4)	N*(1,1)
2	(2,5)	N*(1,1)
3	(3,6)	N*(1,1)
4	(4,7)	N*(1,1)
5	(5,8)	N*(1,1)
6	(6,9)	N*(1,1)
7	(7,10)	N*(1,1)
8	(8,11)	N*(1,1)
9	(9,12)	N*(1,1)
10	(10,13)	N*(1,1)

4. CONCLUSION

The Planned procedure realized here for the Effectual Sharing of Data using Tree based Key Generation provides effective Computational and Communication cost as well as provides more security in comparison to other Frameworks implemented for Key Generation over Pairwise Independent Networks. The Methodology not only generates efficient Keys but also classifies Normal and Attacked Packets in the Network based on the rules generated using Decision Tree

5. REFERENCES

[1] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," Univ. California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb. 2009.

[2] Amazon.com, ―Amazon s3 Availability Event: July 20, 2008,‖ July 2008; http://status.aws.amazon.com/s3-20080720.html

[3] M. Arrington, ―Gmail Disaster: Reports of Mass Email Deletions," Dec. 2006;

[4] T. Ristenpart et al., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security, ACM Press, 2009, pp. 199–212.

[5] Maithili Narasimha and Gene Tsudik. DSAC: integrity for outsourced databases with signature aggregation and chaining. Technical report, 2005.

[6] Joseph, Randy Katz, Above the Clouds: A Berkeley View of Cloud Computing, University of California Electrical Engineering & Computer Science, February 10th, 2009.

[7] Patel, Chandrakant D., Shah, Amip J., "Cost Model for Planning, Development, and Operation of a Data Center," Internet Systems and Storage Laboratory, HP Laboratories, Palo Alto, June 9, 2005.

[8] Alfin Abraham, "An Abuse-Free Optimistic Contract Signing Protocol with Multiple TTPs", IJCA Special Issue on "Computational Science – New Dimensions & Perspectives" NCCSE, 2011.

[9] Giuseppe Ateniese, "Efficient Verifiable Encryption (and Fair Exchange) of Digital Signatures", Proceedings of the 6th ACM conference on Computer and communications security, pp. 138 – 146, ACM 1999.

[10] Guilin Wang. "An Abuse-Free Fair Contract-Signing Protocol Based on the RSA Signature", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 1, March 2010.

[11] F. Bao, G. Wang, J. Zhou, and H. Zhu, "Analysis and improvement of Micali's fair contract signing protocol," in Proc. ACISP'04, vol. 3108, LNCS, pp. 176–187, Springer-Verlag, 2004.

[12] J. Garay, M. Jakobsson, and P. MacKenzie, "Abuse-free optimistic contract signing," in Proc. CRYPTO'99, vol. 1666, LNCS, pp. 449 – 466, Springer-Verlag, 1999.

[13] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 591–606, Apr.2000.

[14] Guilin Wang. "An Abuse-Free Fair Contract-Signing Protocol Based on the RSA Signature", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 1, March 2010.

[15] Lifeng Lai, Siu-Wai Ho," Key Generation Algorithms for Pairwise Independent Networks Based on Graphical Models", IEEE Transactions on Information Theory, 2015.

[16] K. Kalaivani, K. Renugadevi, Nithya," Pairwise Independent Network using Key Generation Algorithm", IOSR Journal of Computer Engineering, 2016.

[17] Sirin Nitinawarat, Chunxuan Ye, Alexander Barg," Secrete Key Generation for a Pairwise Independent Network Model", IEEE Transactions on Information Theory, 2010.

[18] Peng Xu, Zhinguo Ding, Xuchu Dai," The private Key Capacity of a Cooperative Pairwise-Independent Network", 2015.