An Approach of Secure Data Process on Cloud with Effective Monitoring

Priyanka Sharma[1], Nikhar Bhatnagar[2]
[1]Department of Computer Science & Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan Jaipur-302017, (INDIA)
[2]Department of Information Technology, Swami Keshvanand Institute of Technology, Management & Gramothan Jaipur-302017, (INDIA)
Email - priyanka1209sharma@gmail.com
Received 22.06.2019 received in revised form 31.07.2019, accepted 05.08.2019

Abstract : In Cloud figuring, customer can remotely store and recuperate their data reliant on intrigue organization, without the heaviness of close-by data accumulating and upkeep. Nevertheless, the protection of the ordered data arranged and delivered in the midst of the count is transforming into the huge security concern. The rule focus of dispersed figuring enables customers with compelled computational advantages for re-fitting their immense estimation extraordinary main jobs towards cloud, and help to utilized computational power, limit, accumulating, and even appropriate programming that can be shared in a pay per use way. The essential stress of this research is providing the perfect securing data flow with monitoring for any small organization. Here a specify module is to be used for performing the task completing the chain.

Keywords – Cloud, Privacy preserving, Key Generation, IP Generation, Monitoring, Salesforce

1. INTRODUCTION

Distributed computing signifies a noteworthy change the environment in faster manner as to store data and execute the applications. Presently Instead of running projects and information on an individual workstation many organizations want to use it from global location, which is facilitating in the "cloud" a mutual pool of PCs and servers got connection through internet. Distributed computing gives the office to get to every one of the archives and application 27x7 as well location free with enables numerous gathering individuals to team up from various areas. A few frees and solid online capacity administrations accessible to the clients are Microsoft SkyDrive, Apple iCloud, Google Drive, Amazon S3, Dropbox and Gspace.

As the utilization of Cloud computing winds up broad, security of the redistributed client information turns into a critical research subject. It seen that information stockpiling using open cloud while the information activity is always doubtful in private cloud in the mind of organization owner. The parameters are considering for data security as Confidentiality, Integrity, and Availability. The issue of re-appropriating data faces the issues where supplier did not give certification of the security of our data before putting over cloud. Some time when customer is totally relied upon data secured at circulated stockpiling it would be viably gotten. Now the data re-appropriating gathering must offer affirmation to the customer that the data that they have secured on distributed computing [1]. Normally it is to restrict by cloud owners not be changed or balanced by any unapproved customer the stored data. As per study we recognized that hashing technique apply to split the data into fragments. When their fragment is matched then the matched data is recognized.

In this paper, here a better solution is proposed for cloud storage in respect to a secure privacy preserving security [2] of organization important data. This implementation way indicates a secure way for storing data over cloud without any secure communication channels also. The organization users are also did not need to remember the security key generated by organization database because it automatically fetched and execute.

2. LITERATURE REVIEW

2.1 Saidhbi Sheik and Thirupathi Rao Komati (2018)

Cloud computing essentially assumes a job in the part of viable asset use and administration utilization. Regardless of the kind of mists (ex. Private, open, half and half or between cloud), each specialist organizations focuses on the information dwelling in cloud servers. Every single minute, the specialists and researchers are proposing assortment of security calculations to verify cloud information during the exchanges. The vast majority of the cloud information secure calculations are concentrating while in transit to verify to cloud information in a solitary bearing by utilizing cryptographic calculations [3]. In this examination paper centers around another heading to join the highlights of

information pressure with the cloud information so as to verify the cloud information stockpiling.

2.2 Seeza Franklin1 and Prajakta Pravin More (2017)

Salesforce.com is a circulated figuring and social endeavor programming as-an organization (SaaS) provider arranged in San Francisco. It was built up in Walk 1999, in part by past Prophet Official Marc Benioff. Of its cloud stages and applications, the association is acclaimed for its Salesforce customer relationship the administrators (CRM) thing [4], which is include, of Offers Cloud, Administration Cloud, Advertising Cloud, Force.com, Babble and Work.com.

2.3 Cameron Fisher (2017)

As innovation progresses, the abilities of the cutting-edge salesforce keep on advancing. By applying an advanced CRM framework [5], the capacity to oversee selling connections is quickening. This report portrays a scope of ongoing advancements that help a multichannel way to deal with structure profitable client associations.

2.4 Pritam Singh Negi (2016)

This paper introduces the overview on information stockpiling and recovery in distributed computing. In this paper the examination on extension and security issues identified with information stockpiling and data recovery in distributed computing is finished [6]. Information stockpiling and recovery with information security is regular issue in the present situation. The primary target of distributed computing is to empowers clients with constrained computational assets to redistribute their huge calculation outstanding tasks at hand to the cloud.

3. SECURITY ANALYSIS

3.1 Neural Cryptography

In the internet scenario where, identical systems are used in different initial conditions can be synchronized through a common signal. That synchronize depends on time and identical synaptic weights which can be easy executed by cryptography. The secret key is to be share in own private territory. This paper used to generate untold key applied in salesforce module for encryption and decryption.

In this paper the secret key generation procedure is to be executed on the basis of neural networks Hebbian learning rule concept [7]. Where info vector x, a shrouded layer sigma, a loads coefficients w between information vector and the concealed layer which is an initiation system.

$$w_i^{+} = wi + \sigma_i x_i \theta(\sigma_i \tau)\, \theta(\tau^A \tau^B) \quad \ldots\ldots\ldots(1) \qquad \text{(i)}$$

3.2 Secure Count-Min Sketch

Today's when it found that network links are very much counteroffensive for decreasing packet processing. The security of delivered packet needs monitoring for fake and valid packet flow to detection and intrusion prevention. So, the monitoring provides the ensure of encrypted packet to be send and received properly[8] on cloud network flow. Here in this paper I propose a secure version of a updated sketch-based algorithm based on Count-Min which enables to secure traffic monitoring over cloud.

As it seen on network traffic the monitoring task is to track the frequency of IP address by applying the updated Count-Min sketch algorithm's implement hash function will collide with an IP address of associated used. After associated secrete key the packet is to be prevented by the attacker because not able to capable of predicting the nature of packet data. Just by observing the packet attacker not able to recognize the structure having knowledge of monitoring algorithm. Because of the key is unknown to the adversary, it becomes abundantly rigid to attacker to crash.

The proposed algorithm produces an estimate for the value being monitored on a single data structure by searching for the minimum value [9]. The entirety of all estimations is the worth returned by the strategy figures the objective counter to be perused one for every column of the information structure, and afterward restores the base worth found for checking the legitimate and phony IP.

3.3 Hash Functions

No key is utilized in this calculation. A fixed-length hash worth is figured according to the plain content that makes it inconceivable for the substance of the plain content to be recuperated. Hash capacities are additionally utilized by many working frameworks to encode passwords [10].

As per decreases the upkeep cost cloud base implementation with security are become competitive and more useful.

- No need of purchasing licensed software for each system.
- Availability of application 24x7 from any connected internet area from global world improves flexibility.
- Local security make data more secure on web environment
- Network monitoring provide proper checking on web to accept authenticate data[11]
- Keygenrated encypted data is not much prompt to hack
- Not easy to know the data sitting on cloud serve area

3.4 Salesforce

A cloud computing and social endeavor programming as-an administration oversees contact data and coordinates web-based life and continuous client [12]. A module has created for sending the key produced bundle and recovers it by an approved way.

4. PROPOSED ALGORITHMS AND RESULT

There is three-layer security mechanism to be used in this proposed research [13].

1. Key generation: A randomized key value to be generated and store in file.
2. Validity of IP: To save from attacker the packet ip to be checked and only valid packet to be accepted in the cloud storage which monitored by proposed algorithm.
3. Access security: This layer checks the key authentication by created modules for accessed by authorized person.

4.1 Proposed Algorithm

1. Assign value in wid, hei, nip
2. Get a random key in between 1 to 9
3. Create a array of counter with multiplication of wid to hei
4. Execute procedure findkeyhead up to counter value
5. Packet is to forward

Procedure findkeyhead

1. input = <w,d, nip>
2. tCol = rand(key) %width
3. tSlot = tRow + tCol
4. if tr == 0 then
5. rowRes = counter_read("c",tarSlot)
6. break
7. else if rowRes =counter[tarSlot]
8. next check
9. end if
10. result = minimum (result, rowRes)
11. tRow = tRow + width

4.2 Resultant Output of Algorithms

4.2.1 Key generation output

We are generating 4 keys with combination of 20 length stream characters set and special symbols combination using random key generation algorithms executed on Matlab.

temp = 0
t = 0.8418
No. of hidden units = 4
No. of input units = 1
Length of key = 20
No. of iterations = 786
Generated Key =
@@@@@@@@@@@@@@@@@@@@
temp = 0
t = 0.8418 0.4006
No. of hidden units = 4
No. of input units = 2
Length of key = 20
No. of iterations = 464
Generated Key =
DIEACFEC@ECGECFECEDH
temp = 0
t = 0.8418 0.4006 0.8908
No. of hidden units = 4
No. of input units = 3
Length of key = 20
No. of iterations = 787
Generated Key =
EADICDIB@@DGEIBAAFAF
temp = 0
t = 0.8418 0.4006 0.8908 0.7509
No. of hidden units = 4
No. of input units = 4
Length of key = 20
No. of iterations = 534
Generated Key =
FFMICIOPIAGMHFJEGHBD
status = 0

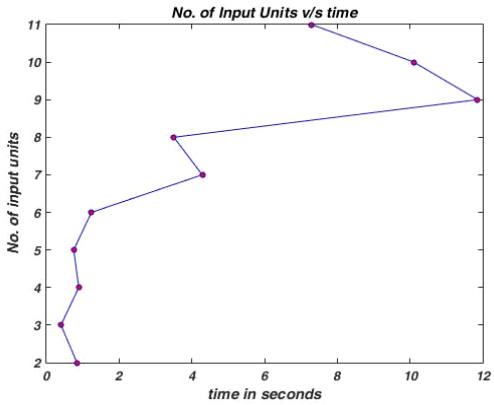

Figure 1: Randomize Key generation graph

4.2.2 Validity of IP check

The error associated with the estimations returned by developed algorithm evaluated in Matlab. Here 4 IP packets are tested as a sample of traffic captured on network's access. The set of randomize packets flow in network distinct monitored by process. Here the sketch for that item's estimated frequency of data packet [14]. The difference between the estimated frequency and its true frequency is the estimation's error.

4.2.3 Module execution result

The generated key which store in file to be access by module. After completing the authentication

process the associated data packet delivered to cloud for storage. Later when retrieval process is to be execute the module check the key to open the data packet. This way a secure process is complete the cycle.

Table 1: Sketch Output

511	911	611	311	111	211	711	411
452	952	152	352	752	552	852	252
633	233	733	833	533	133	333	433
494	694	994	894	794	594	394	294
795	295	695	895	195	995	395	495
646	446	246	346	846	546	146	946
917	317	517	817	117	617	217	717
278	478	778	678	178	578	878	978

Table 2: Counter Output

4	3	5	3	2	2	1	1
3	3	1	3	2	3	2	1
4	3	1	5	2	1	1	1
4	2	2	4	2	1	1	3
1	2	1	2	1	3	2	2
5	2	1	2	1	1	2	2
6	1	2	1	2	2	2	1
4	2	2	1	2	6	1	1

Total No. of error: 4

Table 3: Fake IP

417	417	595	417	0	0	0
0	0	0	0	0	0	0

No. of IP add recd per iteration

6 5 4 3 2

X = 6 5 4 3 2

Y = {7 -1}, {14 -9},{ 10 -6},{ 4 -1},{ 4 -2}

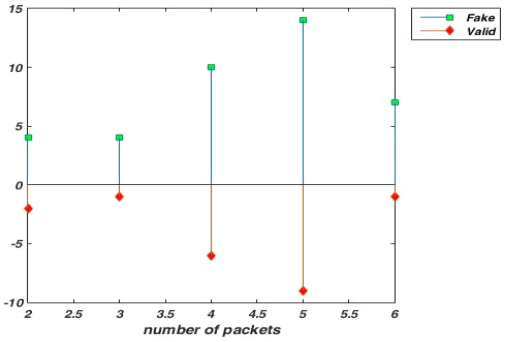

Figure 2: Indication of Fake and valid Data packets

5. CONCLUSION

The proposed approach successfully indicates the secure information transferring and preserving the data on cloud. Here a better security way is to specify as framework. The proposed framework indicates multilayer security as a additionally builds accessibility of client information storing on cloud [15]. Proposed sequential way gives such a useful system structure which achieves input/yield protection, tricking adaptability, and productivity in the cloud as well peace in the mind of organization user.

The flow of research stretched out in future improvement where more security layer can be added. The calculation can be utilized on document, picture and content yet in addition sound and video records. All security layers are working in different stage that will be get successful yield in future.

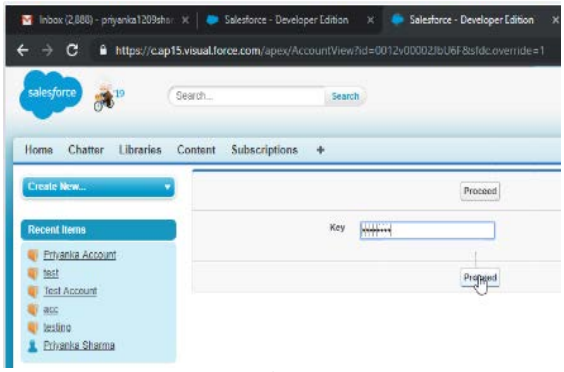

Figure 3: Key placed for executing the process

REFERENCES

[1] P. Nandhini, “A Research on Big Data Analytics Security and Privacy in Cloud, Data Mining, Hadoop and Mapreduce”, Int. Journal of Engineering Research and Appl. (2018), 8, 4, 65-78.

[2] Lin Liu1 and Jinshu Su1 et al., “Privacy-Preserving Mining of Association Rule on Outsourced Cloud Data from Multiple Parties”, Springer International Publishing, LNCS 10946 (2018), 431–451.

[3] Saba Ahmad, M A Azam et al “A Survey on Security And Privacy of Big Data”, International Journal of Engineering Research in Computer Science and Engineering (2018), 5, 4.

[4] Cameron Fisher, “New Technologies for Mobile Salesforce Management and CRM”, American Journal of Industrial and Business Management (2017), vol. 7, 548-558

[5] Seeza Franklin and Prajakta Pravin More, “Salesforce Tool for CRM: A Comparative Study”, International Journal of Current Trends in Engineering & Research (2017), Vol.3 No. 5, 185– 190

[6] Ashutosh Mishra and T M Velayutham, “Fast Data Retrieval and Enhanced Data Security of Cloud Storage in Luby Transform”, Procedia Computer Science (2016), 86-91

[7] K.Saruladha and S.Ranjini “Cogom:Cognitive Theory Based Ontology Matching System”, International Conference on Computational Modeling and Security (2016).

[8] Reddy and K Venkataramana, “Data Mining Technique in Securing the Cloud” Journal of Engineering Research and Application (2018), 8, 3, 1-9.

[9] Seok-Keun Yoo and Bo-Young Kim “A Decision-Making Model for Adopting a Cloud Computing System” Sustainability (2018), 10, 2952.

[10] Kishore Babu and T Paul Kiran et al “Secure Data Storage and Retrieval in the Cloud” SSRG International Journal of Computer Trends and Technology (2017), Issue Special, Pages 127.

[11] R.Sandhya and M.Rekha, “Providing Privacy and Security for Cloud Data Using CANFIS and SCEA Technique”, International Journal Of Current Engineering And Scientific Research (2018), 5, 3, 2351-8104.
[12] Yuling Liu and Hua Peng et al “Verifiable Diversity Ranking Search Over Encrypted Outsourced Data” Tech Science Press CMC (2018), 55, 1, 37-57.
[13] Pritam Singh Negi, “A survey on Data Storage and Retrieval in Cloud Computing”, International Journal on Computer Science and Engineering (2016), 8,7 202-205.
[14] Meng Shen and Guohua Cheng et al. “Content-Based Multi-Source Encrypted Image Retrieval in Clouds with Privacy Preservation” (2018)
[15] Saidhbi Sheik, Data in Cloud Data Storage by Using Cloud Data Compression Mechanism”, International Journal of Recent Technology and Engineering (2018) Vol. 7 No. 452, 49-53.