International Journal of Grid and Distributed Computing
Vol. 13, No. 2, (2020), pp. 440 – 444

Data Slicing and Hybrid Cryptography on Multiple Cloud Storage System

Nouf Saeed Alotaibi
Computer Science Department, Shaqra University, Shaqra, Saudi Arabia
E-Mail: n.saeed@su.edu.sa

Abstract: Cloud security is getting more significant now than any other time in recent memory, however the security for information put away in the cloud has been not ensured still by cloud suppliers. Here, thismanuscript projectsmiddleware, which safely verifies client, scrambles client documents, transfers that to the capacity cloud framework & the other way around. The middleware utilized, cuts the record being transferred into various parts & names it with irregular string, scrambles each divided part with the proposed cross breed cryptographic calculation at that point transfers them into different distributed storage framework. This component of putting away & recovering ensures information security in cloud condition.

Keywords: Hybrid Cryptography, Cloud Computing, Slicing of Data, Security of Cloud.

I. INTRODUCTION

Distributed computing is the on request accessibility of the PC framework assets, particularly information stockpiles & registering power, without direct dynamic administration by the clients. The term is commonly used to depict server farms accessible to numerous clients over the web. Enormous mists, transcendent today, frequently have capacities dispersed over different areas from focal workers. The capacity to upscale & downscale assets as per the clients need is profitable. This is accomplished through appropriate on-request organization, asset pooling & virtualization. The accessibility of high limit systems, ease PCs & capacity gadgets just as the inescapable appropriation of equipment virtualization, administration arranged engineering & autonomic & utility registering has prompted the development in distributed computing.

Distributed storage is a model of PC information stockpiling in which the advanced information is put away in coherent pools. The physical stockpiling traverses numerous workers, & the physical condition is ordinarily possessed & overseen by a facilitating organization. These distributed storage suppliers answerable for keeping the information accessible & available, & the physical condition ensured & running. Individuals & associations purchase or rent stockpiling limit from the suppliers to store client, association, or pertinent information. Distributed storage administrations might be gotten to through an arranged distributed computing administration, a web administration application programming interface or by applications that use the API, for example, cloud work area stockpiling, a distributed storage entryway or Web-based substance the executives frameworks

Cloud computing serves on three models, namely

1. Software as a Service (SaaS)
2. Infrastructure as a Service (IaaS)
3. Platform as a Service (PaaS).

Some of the popular storage cloud systems are:

1) Google Cloud:

Google gives a bound together & solid stockpiling to the web. It permits stockpiling & recovery of any measure of information. There is a free storage available in Google Drive that itself relies on Cloud of Google, it gives document stockpiling & synchronization administration. It gives simple stockpiling & move of client information. The overall applications of Google Slides, Sheets, Photos, Gmail, Docs, Notes, & so on use Google Cloud as their backend stockpiling.

ISSN: 2005-4262 IJGDC

2) AWS S3:

The simple service of storage has been depicts Amazon S3. It could be an article stockpiling administration, which offers huge scope stockpiling. Moreover, it includes straightforward interface, which could be utilized to transfer &download later any measure of information, 24X7 anyplace around globe by means of web. It has its own security framework that gives different confirmation components to make sure about information that is put away in Amazon S3 against unapproved access yet it doesn't ensure information security on entirety. The regular use situations incorporate Backup Storage, Application facilitating, Media facilitating & Software conveyance.

3) Space of Rack:

Space of Rack delivers object stockpiling aimed at records, applications & media on the web. Here, conveys administration internationally at exceptionally high speeds by means of overall substance conveyance arrange. Moreover,could ready for storing any sort of records with no impedimentssize. The space of Rack- framework keeps up 3 duplicates of every document,which were put away clients attain snappier record availability&much solid stockpiling administration. It is controlled by the ground-breaking open source innovation, OpenStack.

4) QNAP:

ONAP gives excellent system connected capacity administration to its clients through web. It utilizes QSync, a cross gadget document synchronization framework to adjust information between the QNAP NAS & different gadgets like work areas, workstations, tablets & cell phones to give adaptable joint effort. Client can store & access any sort of media or archive anyplace & whenever. It additionally gives a versatile application to distantly assume responsibility for information put away in QNAP NAS & remain synchronized.

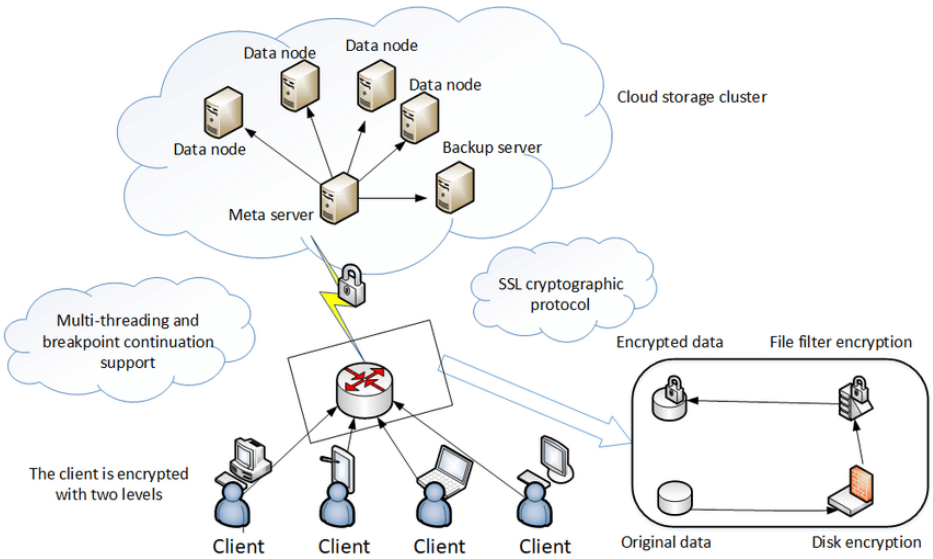

Figure.1. Cloud Storage system Architecture

Since Cloud Computing lay on web, the client information put away in distributed storage frameworks are consistently inclined to security issues like information spillage, information burglary, information adjustment, unauthenticated admittance to information & different programmer assaults. These are generally because of the powerless character the executives, fix the board, hazardous API's & inward & government dangers. Consequently for attaining an overpowered acknowledgment to distributed storage, here, we have projected a middleware framework, which validates client, encodes client records, transfers client information to the capacity cloud & the other way around.

ISSN: 2005-4262 IJGDC

II. LITERATURE REVIEW

Jasleen Kaur & Dr. Sushil Garg, proposes hybrid calculation is a mix of two famous & most generally utilized cryptographic symmetric & topsy-turvy algorithms. It is utilized for confirmation & check reason & Blowfish is utilized for encryption & security reason. Giving verification & non-disavowal of message.Moreover, implies that the recipient gets gotten from sender & furthermore isn't copied. There were 2 keys are utilized aimed at marking record: is left well enough alone with the sender & isn't shared worldwide & subsequently is utilized for marking the archive.

The work in [9], detail clarifies gives, which were looked in distributed computing condition. Moreover, creator thinks of the best possible details & major questions with respect to information. Their answer for The creator contrasts the calculation & different other encryption calculations as far as encryptions every moment utilization to legitimize utilization of AES aimed at making sure about distributed storage. Moreover, thought could just scrambling the information that is put away in distributed is kept up through a divergent physical key administration worker for incorporating security & this ought to be introduced in client's reason.

The work [1], presents a Hybrid Cryptographic computationto protect information security. The framework projected in this manuscript is actualized in eye-OS & crossover calculation conceivable uneven calculation. Moreover, document that should be put away in open cloud could be put away into an impermanent stockpiling & encoded utilizing AES-128, at that point transferred into the distributed storage framework. scrambled utilizing the hilter kilter RSA encryption utilizing the open key & must be private key which is just information proprietor. It could be likewise seen this could be likewise be utilized huge records due to its encryption speed & less utilization of computational asset.

Sidharth Sridhar, ArunMuralidharan, Mohammed Ashik &Vidhya sagar B.S, proposes a middleware which utilizes procedures that includes information cutting & coupling of symmetric & uneven calculation for made sure about & advanced outcomes. Each cryptographic calculation follows both the encryption & decoding measure. The transferred record will be part into different parts & each part is relegated with irregular names. Each part at that point gets scrambled with one of the AES, CAMELLIA & SERPENT calculations & will be put away into cloud. The applied symmetric calculation is & related keys separately. Moreover, record is scrambled with RSA & put away with a similar name as the first document name.To recover the first information from the encoded figure, unscrambling measure is done. To unscramble, the client's suitable private key should be entered, on fruitful private key passage the guide document gets decoded & the framework parses the particular keys for each section from the record, blends the fragments, reproduces the document.

III Proposed System

The projected framework that confirms the client, takes in information from the client, cuts the client information by utilizing a slicer module, allots the cut information to strings which are named haphazardly, & later scrambles the individual strings utilizing any of the three calculations in particular AES,CAMELLIA,SERPENT. After the strings are encoded, they are put away into various cans of a cloud. The applied symmetric calculation is & related keys separately. Moreover, document is scrambled through RSA & put away through a similar name as the first record name. The recovery cycle is like the information inclusion measure, where the information with respect to the instatement, encryption & capacity is spared in a log file.To decode, the client must enter the proper private key,then the guide document gets unscrambled & the framework gives the individual keys for each portion from the record, combines the sections, reproduces the document & makes it accessible for the client. The framework was proposed to improve the security of the cloud information since it is in effect generally utilized by numerous individuals in this day & age.

ISSN: 2005-4262 IJGDC

V. PERFORMANCE ANALYSIS

Here, presentation of framework is assessed dependent on time taken by middleware to transfer & download record to & from distributed storage framework individually

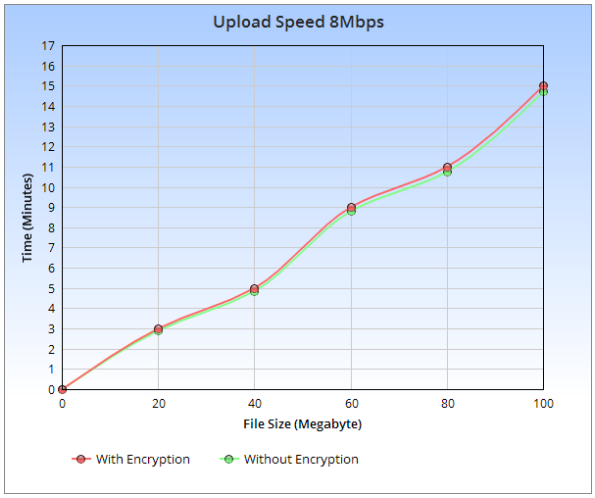

Figure.2. upload time with variable file sizes

From figure 1, absolute execution time taken by middleware is genuinely direct. Minor varieties are available simply because of change in transfer speed. on-off chance that transfer speed is steady, at that point chart would be entirely direct. Likewise, time taken by encryption is calculation minorly affects general execution season of intermediary(system). For instance, to scramble a 100MB record, encryption Algorithms take just 2.5s altogether. complete time taken to transfer incorporates parting documents into different parts, encoding numerous parts, transferring various parts & ace record to cloud. Absolute time for execution for most part depends on transfer speed of ISP.

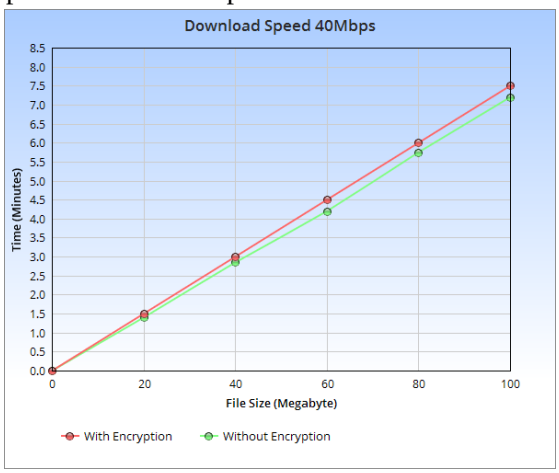

Figure.3. download time with variable file sizes

Since, download speed is steady, we had option to get a direct chart. Moreover, time taken for unscrambling is not exactly time taken for encryption in light of prior keys & introductory vectors (No compelling reason to produce arbitrary keys & beginning vectors once more). re isn't a lot of variety in an ideal opportunity for records transferred with & without encryption. For downloading record with unscrambling, it takes around 7.5s & for downloading document with no decoding it takes around 7.2s. This time additionally incorporates an opportunity to unscramble & converge to reproduce first record.

ISSN: 2005-4262 IJGDC

variety may appear to be observable if document size is huge, however higher security comes to detriment of greater expense.

CONCLUSION

The objective of this manuscript projected a novel kind of security cloud storage method, where DATA SLICING & use of HYBRID CRYPTOGRAPHY takes place. Data that is being sent, is sliced, encrypted &stored in different buckets of cloud storage. This helps in data security a lot as re are three algorithms which are being used in this middleware which prevents attackers from accessing entire user data. Data is also stored in randomly named strings that prevents attacker from recognizing pattern. User has a private key which is & this ensures safety of cloud data. Middlewarefor access log filethat enhances total security of cloud storage devices. Future works involve improving response time of system& also making it work in a decentralized environment.

REFERENCES

1. Sidharth Sridhar, ArunMuralidharan, Mohammed Ashik &VidhyasagarB.SEnhanced Cloud Storage Security using Data Slicing & Hybrid Cryptography.
2. DivyaPrathana Timothy &Ajit Kumar Santra, "A Hybrid Cryptography Algorithm for Cloud Computing Security" IEEE Publication, 2017.
3. Rajiv Mishra, MeenaxiKumari (2015), "Need of Multi-Layer Security in Cloud Computing for on Dem& Network Access", International Journal of Computer Science & Mobile Computing (IJCSMC), Vol. 4, pp. 398 – 404.
4. Lovejeet Kamboj, PawanLuthra (2017) "Multi-Layer Data Security in Cloud Computing", International Journal of Computational Engineering Research (IJCER), Vol. 7, pp. 1
5. Vishwanath S Mahalle&Aniket K Shahade, "Enchancing Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm" IEEE Publication, 2014.
6. Jasleen Kaur & Dr. Sushil Garg, "Security in Cloud Computing using Hybrids of Algorithms" International Journal of Engineering Research & General Science Volume 3, Issue 5, September-October 2015.
7. Kumar, K. Vijay, B. Srinivas Reddy & Dr. N. Ch&raSekhar Reddy, "Preserving Data Privacy, Security Models & Cryptographic Algorithms in Cloud Computing" International Journal of Computer Engineering & Applications, 2015.
8. Deyan Chen & Hong Zhao, "Data Security & Privacy Protection Issues in Cloud Computing" IEEE International Conference on Computer Science & Electronics Engineering, 2012.
9. R. Kiruthuka, S. Keerthana& R. Jeena, "Enchancing Cloud Security using AES Algorithm" International Journal of Advanced Research in Computer Science & Software Engineering, Volume 5, Issue 3, March 2015.
10. Dr. N&itaSengupta, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security", International Journal of Innovative Research in Computer & Communication Engineering, Volume 3, Issue 5, May 2015.
11. Hanumantha Rao, Galli & Dr. P. Padmanabhan, **"**Data Security in Cloud using Hybrid Encryption & Decryption**"** International Journal of Advanced Research in Computer Science & Software Engineering, Volume 3, Issue 10, October 2013.
12. S. Munjal1 & S. Garg, "Enhancing Data Security & Storage in Cloud Computing Environment" IJCSIT, Volume 6, 2015.
13. ShiroleBajirao& Dr. Sanjay Thakur, "Data Confidentiality in Cloud Computing with Blowfish Algorithm" International Journal of Emerging Trends in Science & Technology, IJETST, Volume 1, Issue 1, March 2014.