JES
Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

FORMULATING A SECURITY LAYER WITH EFFICIENT DATA COLLECTION AND COMPUTATIONAL INTELLIGENCE IN FOG COMPUTING

[1]Rashida Tasneem Habeeb, [2]K. Shilpa
[1]PG Scholar, MTech, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.
tasneemhabeeb9966@gmail.com
[2]Asst Professor, Dept of IT, Shadan Women's College of Engineering and Technology HYD, T.S.

ABSTRACT— Ongoing years witness the improvement of distributed computing innovation. With the touchy development of unstructured information, distributed storage innovation improves advancement. In any case, in current stockpiling pattern, client's information is completely put away in cloud servers. As it were, clients lose their privilege of control on information and face security spillage ris. Conventional security assurance plans are typically founded on encryption innovation, yet these sorts of techniques can't adequately oppose assault from within cloud server. So as to take care of this issue, we propose a three-layer stockpiling system dependent on haze processing. The proposed system can both exploit distributed storage and secure the protection of information. In addition, Hash-Solomon code calculation is intended to separate information into various parts. At that point, we can put a little piece of information in nearby machine and mist server so as to ensure the protection. Additionally, in light of computational insight, this calculation can register the dissemination extent put away in cloud, mist, and neighborhood machine, separately. Through the hypothetical security investigation and test assessment, the attainability of our plan has been approved, which is extremely a ground-breaking supplement to existing distributed storage conspire.

Index Terms—Cloud computing, cloud storage, fog computing, privacy protection.

I.INTRODUCTION

SINCE the 21st century, PC innovation has grown quickly. Distributed computing, a developing innovation, was first proposed in SES 2006 (Search Engine Strategies 2006) by San Jose and characterized by NIST (National Institute of Standards and Technology) [1]. Since it was proposed, distributed computing has pulled in extraordinary consideration from various parts of society. Distributed computing has continuously developed through such a large number of individuals' endeavors [2]. At that point there are some cloud-based advances getting from distributed computing. Distributed storage is a vital piece of them.

With the quick advancement of system transfer speed, the volume of client's information is rising geometrically [3]. Client's necessity can't be fulfilled by the limit of local machine any more. Thusly, individuals endeavor to discover new techniques to store their information. Seeking after progressively incredible capacity limit, a developing number of clients select distributed storage. Putting away information on an open cloud server is a pattern later on and the distributed storage innovation will wind up broad in a couple of years. Distributed storage is a distributed computing framework which gives information stockpiling and the board administration. With a group of utilizations, arrange innovation and disseminated record framework innovation, distributed storage makes a substantial number of various stockpiling gadgets cooperate coordinately [4], [5]. These days there are a great deal of organizations giving an assortment of distributed storage administrations, for example, Dropbox, Google Drive, iCloud, Baidu Cloud, and so on. These organizations give vast limit of capacity and different administrations identified with other well known application, which thusly prompts their accomplishment in pulling in amusing endorsers. Be that as it may, distributed storage administration still exists a great deal of security issues. The protection issue is especially critical among those security issues. Ever, there were some renowned distributed storage protection spillage occasions. For instance, Apples iCloud spillage occasion in 2014, various Hollywood performers private photographs put away in the fogs were stolen. This occasion caused mayhem, which was in charge of the clients' tension about thae security of their information put away in cloud server.

As appeared in Fig. 1, client transfers information to the cloud server straightforwardly. Thusly, the Cloud Server Provider (CSP) will occur of client to deal with the information. In outcome, client doesn't really control the physical stockpiling of their information, which results in the division of possession and the executives of information [6]. The

CSP can unreservedly access and pursuit the information put away in the cloud. In the interim the aggressors can likewise assault the CSP server to acquire the client's information. The over two cases both make clients fell into the peril of data spillage and information misfortune. Conventional secure distributed storage answers for the above issues are generally concentrating on access confinements or information encryption. These strategies can really wipe out most piece of these issues.

Not with standing, these arrangements can't illuminate the inward assault well, regardless of how the calculation improves. There-fore, we propose a TLS conspire dependent on fog computing model and plan a Hash-Solomon code dependent on Reed-Solomon code [7], [8]. Fog computing is an all-inclusive registering model dependent on distributed computing which is made out of a ton of fog nodes. These nodes have a specific stockpiling limit and preparing capacity. In our plan, we split client's information into three sections and independently spare them in the cloud server, the fog server and the client's local machine. In addition, contingent upon the property of the Hash-Solomon code, the plan can guarantee the first information can't be recuperated by fractional information. On another hand, utilizing Hash-Solomon code will create a part of repetitive information squares which will be utilized in deciphering technique. Expanding the quantity of excess squares can build the unwavering quality of the capacity, however it likewise results in extra information stockpiling. By sensible distribution of the information, our plan can truly secure the protection of client' information. The Hash-Solomon code needs complex figuring, which can be helped with the Computational Intelligence (CI). Ideal models of CI have been effectively utilized as of late to address different difficulties, for instance, the issues in Wireless sensor systems (WSNs) field. CI master vides versatile instruments that display shrewd conduct in mind boggling and dynamic situations like WSNs [9]. In this way in our paper, we exploit CI to do some figuring works in the fog layer. Contrasted and conventional techniques, our plan can give a higher security assurance from inside, particularly from the CSPs.

II. RELATED WORKS

The significance of security in distributed storage has pulled in a great deal of consideration regardless of in academe or industry. There are a ton of examines about secure distributed storage structures as of late. So as to unravel the security issue in distributed computing, paper [10] proposed a protection safeguarding and duplicate discouragement CBIR plot utilizing encryption and watermarking methods. This plan can ensure the picture substance and picture includes well from the semi-legit cloud server, and dissuades the picture client from unlawfully circulating the recovered pictures. Shen et al. think cloud is semi-trusted and propose a system for urban information sharing by abusing the characteristic based cryptography. The plan they proposed is secure and can oppose conceivable assaults [11]. Fu et al. propose a substance mindful pursuit conspire, which can make semantic hunt progressively brilliant. The examinations results demonstrate that their plan is productive [12].

SECURE CLOUD STORAGE BASED ON FOG COMPUTING

The security degree is a basic estimation to measure the idea of dispersed stockpiling structure. Additionally, data security is the most fundamental part in circulated stockpiling security and it fuses three points: data insurance, data uprightness and data openness. Ensuring data assurance and dependability has constantly been the point of convergence of relevant asks about [26]. On another hand, data security is also the most concerned bit of the customers. From a business for each spective, association with high security degree will attract more customers. Along these lines improving security is a basic goal no tangle ter in the academic world or business. Around there, we will detailedly extend how the TLS structure verifies the data insurance, the utilization nuances of work process and the speculative prosperity and efficiency examination of the limit plot.

A. Fog Computing

Our plan depends on fog computing model, which an expansion of cloud is registering. Fog computing was right off the bat proposed by Ciscos Bonomi in 2011 [27]. In Bonomi's view, fog computing is like the distributed computing, the name of fog computing is striking. Contrasted with very focused distributed computing, fog computing is nearer to edge arrange and has numerous points of interest as pursues: more extensive topographical appropriations, higher ongoing and low inactivity. In considering of these characters, fog figuring is progressively appropriate to the applications which are touchy to delay. On another hand, contrasted with sensor nodes, fog computing nodes have a specific stockpiling limit and information handling capacity, which can do some basic information preparing, particularly those applications dependent on geological area. In Fog computing is normally a three-level design, the highest is distributed computing layer which has

incredible capacity limit and register ability. The following dimension is fog computing layer. The fog computing layer fills in as the center layer of the fog computing model and assumes a urgent job in transmission between distributed computing layer and sensor organize layer. The fog nodes in fog computing layer has a specific stockpiling limit and process capacity. The base is remote sensor arrange layer [28]. The principle work of this layer is gathering information and transferring it to the fog server. In addition, the exchange rate between fog computing layer and different layers is quicker than the rate legitimately between cloud layer and the base layer [29]– [31]. The presentation of fog computing can help the distributed computing layer, improving the work effectiveness. In our plan, we exploit the fog computing model, adopt three-layer structure. Moreover, we supplant the WSNs layer by client's local machine.

B. Three-Layer Privacy Preserving Cloud Storage Scheme Based on Fog Computing Model

So as to secure client's protection, we propose a TLS outline work dependent on fog computing model. The TSL structure can give client a specific intensity of the board and successfully ensure client's security. As referenced, the inside assault is hard to stand up to. Conventional methodologies function admirably in understanding outside at-tack, however when CSP itself has issues, customary ways are altogether invalid. Not the same as the conventional methodologies, in our plan, client's information is partitioned into three diverse size parts with encoding innovation. Every one of them will do not have a piece of key data for classification. Consolidating with the fog computing model, the three pieces of information will be put away in the cloud server, the fog server and client's local machine as per the request from huge to little. By this strategy, the aggressor can't recuperate the client's unique information regardless of whether he gets every one of the information from a specific server. Concerning the CSP, they likewise can't get any valuable data without the information put away in the fog server and local machine in light of the fact that both of the fog server and local machine are constrained by clients.

As appeared in Fig. 2, the TLS structure makes full utilization of fog server's stockpiling and information preparing ability. The engineering incorporates three layers, the cloud server, the fog server and the local machine. Every server spares a specific piece of information, the capacity extent is dictated by clients' assignment system. Initially, client's information will be encoded on client's local machine. At that point, for instance, let 1% encoded information be put away in the machine. At that point transfer the rest of 99% information to the fog server. Besides, on the fog server, we do comparable activities to the information which originates from client's machine. There will be about 4% information put away in the fog server and afterward transfer the rest of to the cloud server. The above tasks depend on Hash-Solomon code. Hash-Solomon code is a sort of coding techniques dependent on Reed-Solomon code.

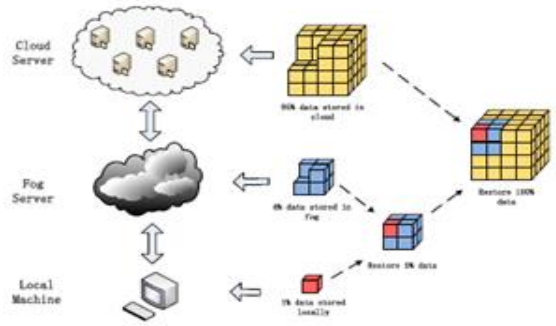

Fig. 1 Illustration of Three-Layer storage framework based on fog computing.

Subsequent to being encoded by Hash-Solomon code, the information will be partitioned into k parts and produces m repetitive information. Hash-Solomon code has such property, in these k+m parts of information, in the event that somebody has in any event k parts, he can recuperate the total information. In other word, it's not possible for anyone to recuperate the complete data with not as much as k parts of information. As indicated by this property of Hash-Solomon code, in our plan, we let close to k-1 parts of information be put away in higher server which has larger storage limit and given the rest of chance to be put away in the lower server. Along these lines, the stealer can't recoup the total information regardless of whether one of the three layers' information was stolen. In this way we can guarantee the security of client's information. At that point we think about the estimation of k and m. Accepting that we need to spare r% information on the fog server. In the Hash-Solomon code, we have definitions as data blocks to the number of data blocks which will be used in encoding. In other words, the ratio of the number of data blocks stored in lower server to the number of data blocks stored in the upper server. For example, the ratio of the number of data blocks stored in the local machine to the number of data blocks stored in the fog server. In the same way, the ratio of the number of data blocks stored in the fog server to the number of data blocks stored in the cloud server.

Definition 2 Maximal Invalid Ratio: the maximal invalid ratio is the ratio of the number of invalid data to the number of all data blocks when the upper server can just recover the complete data by the data blocks stored in them. If there was one more
The parameter k is the number of blocks after data being divided, the parameter m is the number of redundant data blocks and the parameter r is the storage ratio of different servers. Be- sides, the fog server includes Computational Intelligence which can help the system with calculating the results of the values of k and m, because of the nodes in the fog server having its own computing power.

C. Implementation Detail of Workflow

1)Stored Procedure: When user wants to store his file to the cloud server, the procedure is shown as Fig. 3. First of all, user's file will be encoded with Hash-Solomon code. And then, the file will be divided into several data blocks and the systems will also feedback encoding information simultaneously. Assuming that 1% data blocks and the encoding information will be stored locally. The remainder 99% data blocks will be uploaded to the fog server. Secondly, after receiving the 99% data blocks from user's machine, these data blocks will be encoded with Hash- Solomon again.

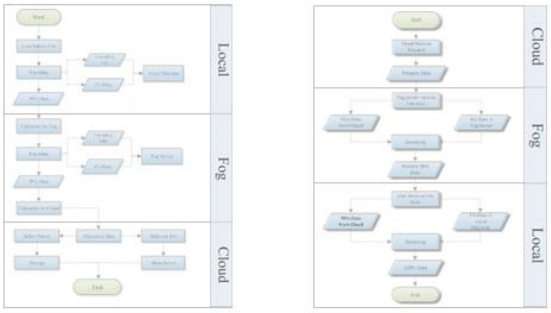

Fig. 2. Diagram of stored procedure.

These data blocks will be divided into smaller data blocks and generates new encoding information. Similarly, assuming that 4% data blocks and encoding information will be stored in the fog server. The remainder 95% data blocks will be uploaded to the cloud server. Thirdly, after cloud server received the data blocks form fog side, these data blocks will be distributed by cloud manage system [32]. Finally, the storage procedure ends when all the related information be recorded in different servers.

2) Download Procedure: When user wants to download his file from the cloud server, the procedure is shown in Fig. 4. Firstly, cloud server receives user's request and then integrates the data in different distributed servers. After integration, cloud server sends the 95% data to the fog server. Secondly, the fog server receives the data from the cloud server. Combining with the 4% data blocks of fog server and the encoding information, we can recover 99% data. Then the fog server returns the 99% data to the user. Thirdly, the user receives the data from fog server. User can get the complete data by repeating the above steps.

D. Theoretical Safety Analysis

This section will provide theoretical safety analysis of the structure proposed in our research and prove that the secure storage structure can really improve the capability of privacy protection

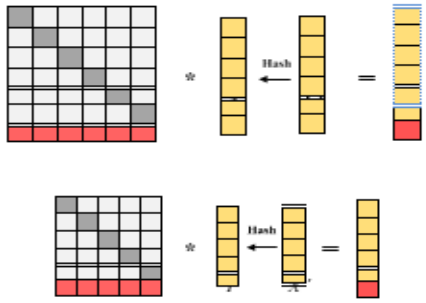

Fig. 3. Diagram of download procedure.

Based on the Reed-Solomon code algorithm, we propose a Hash-Solomon code algorithm. The Hash-Solomon encoding process is actually a matrix operation. As shown in Fig. 5, firstly we should do mapping transformation on the file which is prepared to be stored, so that each word of the file corresponds to a number in GF (2ω) After mapping transformation we get file matrix O. Secondly we do hash transform on matrix O and get matrix X. Then we multiply the transformed matrix X by the encoding matrix A.

III. RESULT

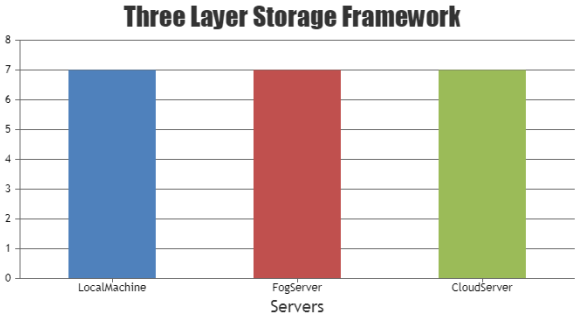

Fig 4. Three Layer Storage Framework

IV. CONCLUSION

The expansion of distributed-Computing presents on the method to us a ton of advantages. circulated storage be an advantageous innovation which encourages clients to expand their capacity limit. Be that as it may, distributed-storage additionally causes a growth of secure issues. When utilizing distributed storage, clients don't really manage the substantial stockpiling of them in sequence with it consequences in the separation of possession and the executives of data-information. So as to look after of the issue of security assurance in distributed storage.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Com- mun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.

[4] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.

[5] Y. Li, T. Wang, G. Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.

[6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[8] J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[9] R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelli- gence in wireless sensor networks: A survey," IEEE Commun. Surv. Tuts., vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy- preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[11] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive Mobile Comput., vol. 41, pp. 219–230, 2017.

[12] Z. Fu, F. Huang, K. Ren, J. Weng, and C. Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.

[13] Q. Hou, Y. Wu, W. Zheng, and G. Yang, "A method on protection of user data privacy in cloud storage platform," J. Comput. Res. Develop., vol. 48, no. 7, pp. 1146–1154, 2011.

[14] P. Barham et al., "Xen and the art of virtualization," ACM SIGOPS Oper. Syst. Rev., vol. 37, no. 5, pp. 164–177, 2003.

[15] G. Feng, "A data privacy protection scheme of cloud storage," vol. 14, no. 12, pp. 174–176, 2015.