International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 22 (2015) pp 43177-43181
© Research India Publications. http://www.ripublication.com

Bio inspired Ferret Auditing Technique (FAT) for Cloud Computing

S. Tejaswini

SITE, VIT University, INDIA tejusunder@yahoo. in

D. Akshay Kumar

SITE, VIT University, INDIA dhupamakshay. kumar@gmail. com

K. Indu Prudhvi

SITE, VIT University, INDIA prudhvikolipaka@yahoo. com

Abstract

Cloud computing is a radical and impending technology. It is obliging in tidying away large volume of data. The data stored might be very confidential so integrity of data is very important, hence Cloud security is one of our main concerns, to overcome these security challenges we adopt auditing technique. Auditing process is done in a regular basis to check the integrity of the data uploaded by the client. Many auditing process exist, they trail the traditional method of scrutinizing large amount of data but they are of dawdling nature. It normally takes a long time auditing data, this fashion. To overcome the time complexity we come up with a Ferret Auditing Technique(FAT), by implementing this, the critical files needed by the client can be searched quickly, to do this we have come out with a heuristic search based auditing creating a meta cloud where tags are stored. The technique uses A* algorithm to retrieve the tags from the tag cloud bio-inspired by filter feeding technique adopted by blue whales and a catch nest concept followed by owls to store food needed the most. This bio inspiration lead us come up with a modified heuristic search based auditing. By instigating this algorithm we achieve time constrained auditing with data integrity.

Keywords— Cloud Security, Auditing Techniques, Heuristic Search, Time Constrained.

I. INTRODUCTION

Cloud-computing technology has been developing rapidly now-a-days. Computing resources are pooled together to serve multiple clients at the same time[ ]. Patrons can rent the necessary resources as long as they stand in need of, and they can access it anywhere, any time. Application run on hosted servers as service in cloud. As the cloud computing evolution nurtures, security challenges have been growing rapidly. In order to enhance security measures, a third party auditor services has been introduced or [conceded] to verify the dynamically uploaded data periodically and report the status to data owners without demanding any local copy of data. An auditor can audit multiple data uploaded by different users which is called as batch auditing. But this may not satisfy data integrity, security at all times. Verifying whether the data information remains intact during the data modification or updation is called data integrity. Eventually computation may take a longer time in batch auditing since the auditing has to be performed simultaneously on the data required.

In order to achieve data integrity and security in [4] have proposed techniques including polynomial –based authentication tags and holomorphic linear authenticators. To achieve privacy –preserving public cloud data auditing [1] uniquely combine the public key based holomorphic authenticator with random masking. Implementing this technique they achieved batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by [Third Party Auditor [TPA]. To achieve consistency as a service in cloud auditing [2] follows a two layered cloud auditing architecture in which two layers are connected by loosely synchronized clock. Each user can perform local auditing independently; this operation focuses on monolithic-read, read-your-write consistency. Global auditing focuses on casual consistency which is performed by constructing a direct graph; if the graph is acyclic the casual consistency is preserved. Cohesion violations and staleness of the value of read are calculated and heuristic auditing strategy (HAS) is used to check and reveal as many violations possible. To achieve security [5] forensics service oriented architecture which audit framework towards a Forensic-based Service Oriented Architecture (FOA) Framework for Auditing of Cloud Logs. Once the construction block is done this system can be used for security and assurance for cloud empowered (SOA). This actually reduces the confidence of potential attackers. They have also built a complete manual data Centre investigation, which is supported by developing Web services.

In our paper, we propose a mechanism of generating a tag for every data block that has been uploaded by data owners which is used by an auditor for tracing the data in cloud. Each tag generated will have a unique format making it more secure. These tags are stored separately in other cloud called as a Tag Cloud.

In real-world applications, heuristics play a vital role in resolving complex problems, search strategies. Heuristic rules can be used for detecting viruses and other variety of malware. Heuristic scanning predicts the code and/or behavioral patterns which indicates the class or family of viruses. Main motive of implementing heuristic is that, it provides with a minimized, time sinking methodology which can be easily used for any searching process or intricate, unresolvable problems. Heuristics is used to optimize the algorithm for its efficient execution.

A* algorithm is efficient to search the required data reducing the time complexity for searching process. We propose a modified heuristic A* algorithm, Ferret auditing technique[FAT] which has been enthused from the bio inspiration technique “filter feeding”, followed by blue whale.

Even though blue whale does not have teeth, they are carnivorous. Every day an adult blue whale consumes about four tons of small shrimp-like organisms. In order to eat, a blue whale takes large gulps of water, extending its frilled throat. The whale filters the water by shoving its huge tongue and contracting its throat, technique which has been inspired an used to modify the traditional A* algorithm. We have also use a cache nest concept used by owls which stores food which it needs the most in a separate place and access it very easily. By instigating our algorithm we can achieve enhanced security for data, reducing time complexity and computation overhead.

II. RELATED WORKS

Jiawei Yuan et al. [4] proposed the first public and constant cost storage integrity auditing scheme with secure deduplication (PCAD) scheme which enables the deduplication of both files and their corresponding tags, and thus substantially save computation cost and communication cost for multiple request scenario. This scheme efficiently handles multiple auditing requests with batch operations. Author Qin Liu et al discuss about the “consistency as a service “auditing concept in their paper [2]. Here basically they have one main cloud model called the consistency as a service which is directly maintained by a cloud service provider and they have group of users in the audit cloud where they act as auditors directly to maintain the integrity of their data. This is a two-level auditing architecture. It is simple and the clouds are lightly connected by the synchronized clock. Each user can perform local auditing independently; this operation focuses on monolithic-read read-your-write consistency. Global auditing focuses on casual consistency which is performed by constructing a direct graph; if the graph is acyclic the casual consistency is preserved. Cohesion violations and staleness of the value of read are calculated and heuristic auditing strategy (HAS) is used to check and reveal as many violations possible. In [8]-[11] they have discussed about the security and integrity attacks of data in cloud and proposed their techniques to overcome those issues. Author Sean Thorpe and ET en al[5] discuss about “Forensic-centered Service Oriented Architecture Organization for Auditing of Cloud Logs. Cloud computing log digital investigation is similar to investigation of a potential crime using digital forensic evidence from a virtual machine using the hyper vision event cloud. A data cloud log which is forensics service oriented architecture (SOA) audit framework towards a Forensic-based Service Oriented Architecture (FOA) Framework for Auditing of Cloud Logs. Once the construction block is done this system can be used for security and assurance for cloud empowered (SOA). This actually reduces the confidence of potential attackers. They have also built a complete manual data Centre investigation, which is supported by developing Web services which records potential evidences. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou utilized and uniquely combined the public key based homomorphic authenticator and random masking to achieve privacy-preserving public cloud data auditing system[1]. They have proved that their scheme is suitable for batch auditing and is mainly based on four algorithms and two phases by which eventually we can preserve data security. Boyang Wang, Baochun Li, et al [7] discussed about the mechanism that supports public auditing on shared data stored in the cloud. They have come up with a novel idea to verify shared data integrity without retrieving the complete data. Qian Wang, Cong Wang, Kui Ren [3] Manipulated the classic Merkle Hash Tree construction for block tag Authentication. They have proved that their technique is secure and highly efficient by performance analysis. Rathore, H. ; Badarla, V[11] proposed a technique inspired by human immune system. They have compared the being of human body under pathogenic attacks with the analogies between network security.

III. PROPOSED WORK

In a traditional cloud environment, the shared data and its verification metadata (i. e. signatures) are both stored in cloud server. A public verifier, such as a third-party auditor (TPA) provides the expert data auditing service. When a public verifier wishes to check the data he has to send an auditing challenge to the cloud server [7]. After receiving the auditing challenge the cloud server sends an auditing proof of the possession of the stored data, and then the verifier checks the correctness of the data with the help of auditing proof. Although they achieve verification of shared data without verifying the whole cloud data, the data to be searched other than the shared, it follows the normal search process. Another drawback is the data is uploaded by an original user it is accessible to the group users also they also can modify the data.

Literature survey reveals several limitations found in existing auditing systems in terms of search time complexity, privacy and role breaches. To overcome this we propose Ferret Auditing Technique (FAT). The data uploaded by the cloud user/client is primarily broken into blocks and stored in the cloud. When the data is divided, a unique tag will be assigned for each and every data block generated. The length of the generated alpha numeric format of tag is 28 characters and size of a tag is 98 bytes, which is much less than the size of actual data, making the auditing process convenient and reduces the time complexity for searching the particular data that has to be audited from a bulk of data which was uploaded

Every tag reflects the data stored in cloud. User code contains the first three letters of the user’s registered name, designation level has two characters of the designation the user belongs to, upload id and the download id are single flag values which signifies whether the data has been uploaded or downloaded. Next eight characters represent the date it has been uploaded and the successive four characters represent the time the user logged in. The next six integers represent the size of the data. Colors are assigned to the tags generated. The tags will be assigned with lighter colors which are retrieved for a less number of times and are assigned with brighter colors which are retrieved for a more number of times. The tag will be generated with a unique format of alpha numeric code. Each tag is stored in a hierarchical way in specified alphabet tree of the tag Cloud. All the tags are stored in the tag cloud making the auditing process faster and simpler for the data auditor. Now we use the modified A* heuristic search algorithm, Ferret auditing Algorithm which has been derived from bio – inspiration to find the particular tag in the tag cloud for the secure auditing process of the required data. If the data matches the verification process is complete, within a short period of time.

The conception of bio inspired heuristic A* search algorithm is derived from a bio inspiration where the blue whale follows the filter feeding technique and the tag cloud concept taken from the owl which has a cache nest where food needed the most is stored. By implementing this technique the data uploaded by the client is not revealed making it more secure, auditing is done based on tags generated. since the tags stored are of less memory space, time complexity for auditing process can be reduced, hence an effective heuristic search based auditing can be achieved.

A* algorithm works similar to Dijkstra algorithm in worst case. But in concrete cases it works more efficiently, by searching in a precise[particular] direction. It will be computed in O[1]time.

FAT always selects the path from the souce node to the target with lowest value of h(v)+D[v](D[v]-estimates distance from source to nearest node and h(v)-calculates distance from source to the target), instead of the one with only the lowest value of the distance from source to the nearest node. This tends to select path not to the node that is closest to source, but the one that will be the shortest path to the target.

Then Tags generated will be stored in the trees in an alphabetical order. only 26 trees[26 alphabet trees, each tree represents a particular alphabet], reducing the time complexity for searching process. When any tag has to be searched, our algorithm directs automatically to a particular alphabet in the alphabet tree which matches with the first letter of the tag format. Then tree where the first letter is identical for example if it is "a" then it should be directed to the particular alphabet tree.

our algorithm filters the paths at each level and drives to the other level in the direction of the target which is inspired by blue whale "filter feeding". while in Bfs, Dijsktra it will calculate all the possible paths from its source to the destination which is time consuming.

But by implementing our modified, bio inspired A* algorithm, we can reach the target within less time compared to other algorithms.

User code	Designation level	Upload id	Download id	Sys date	Sys time	Size of data	Number of times accessed w. r. t colors

User code-first three letters of user name.
Designation level-The designation of the user.
Upload id-It is a flag, represents whether the data is uploaded.
Download id-It is a flag, represents whether the data is downloaded.
Sys date-Date the data has been uploaded.
Sys time-Time user has been logged-in.
Size of data-Size of the data that has been uploaded.

Fig. 1. Format of the Tag

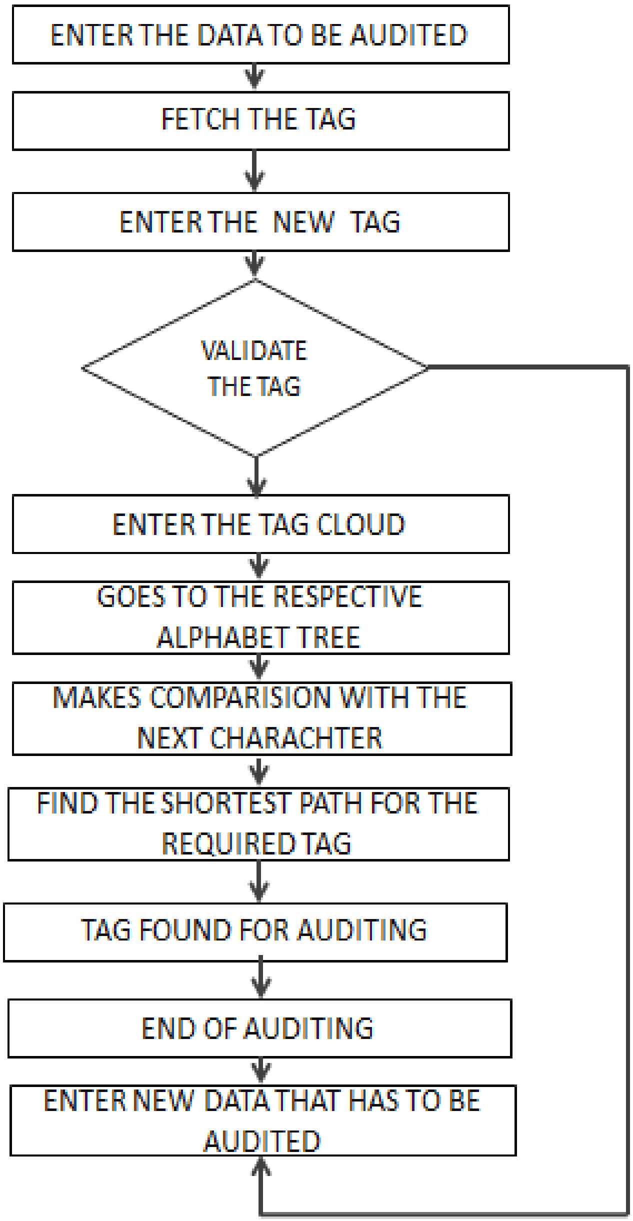
ENTER THE DATA TO BE AUDITED
FETCH THE TAG
ENTER THE NEW TAG
VALIDATE THE TAG
ENTER THE TAG CLOUD
GOES TO THE RESPECTIVE ALPHABET TREE
MAKES COMPARISION WITH THE NEXT CHARACHTER
FIND THE SHORTEST PATH FOR THE REQUIRED TAG
TAG FOUND FOR AUDITING
END OF AUDITING
ENTER NEW DATA THAT HAS TO BE AUDITED

Fig. 2. Algorithm

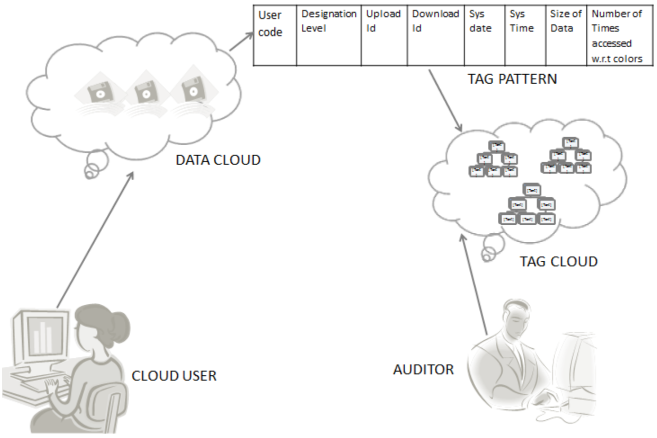

Fig. 3. Architecture diagram

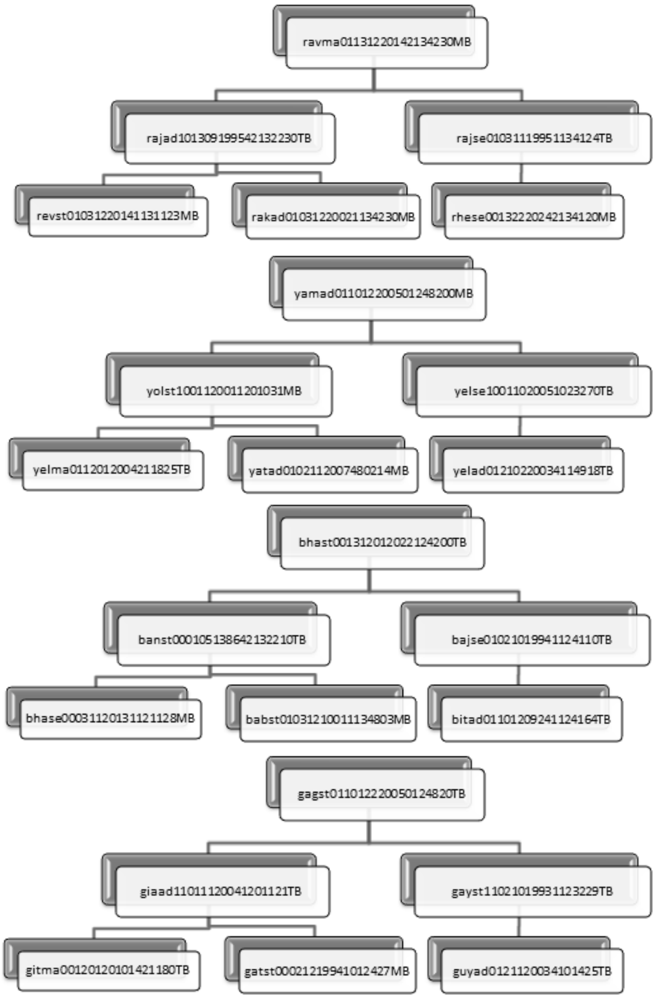

Fig. 4. Tags stored in a hierarchical way in tag Cloud

IV. CONCLUSION

From the comparison of the normal auditing with our bio inspired heuristic search auditing we can clearly understand that we follow a unique method in auditing the data which incorporates speed, reducing time complexity and selecting a particular data for auditing which is not conceivable in other auditing methods. Our algorithm is developed on the bases of filter feeding technique where we use a* algorithm to search the data and retrieve the data precisely and in a less amount of time. Implementing Ferrit Auditing Technique [FAT], the auditor can search a particular data which he wants to audit. The flow chart which was shown in fig. 2 will clearly depicts how the algorithm works. The data uploaded by the user is also very secure as for each data block uploaded by the user, a tag will be generated with an alphanumeric code [with a unique format] and stored in a hierarchical way in a separate cloud. so the auditor uses only the tag cloud to audit the data in the data cloud in very safe. Hence our proposed work has overcome the security and time constraint problems and enhanced heuristic search auditing. We have come up with only the basic algorithm, we have to work on real implementation of this in cloud.

V. REFERENCES

[1] Cong Wang; Qian Wang; Kui Ren; Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, " INFOCOM, 2010 Proceedings IEEE, vol., no., pp. 1, 9, 14-19March2010

[2] Liu, Q. ; Wang, G. ; Wu, J., "Consistency as a Service: Auditing Cloud Consistency, " Network and Service Management, IEEE Transactions on, vol. PP, no. 99, pp. 1, 11

[3] Qian Wang; Cong Wang; Kui Ren; Wenjing Lou; Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, " Parallel and Distributed Systems, IEEE Transactions on, vol. 22, no. 5, pp. 847, 859, May 2011

[4] Jiawei Yuan; Shucheng Yu, "Secure and constant cost public cloud storage auditing with deduplication, " Communications and Network Security (CNS), 2013 IEEE Conference on, vol., no., pp. 145, 153, 14-16 Oct. 2013

[5] Thorpe, S. ; Grandison, T. ; Campbell, A. ; Williams, J. ; Burrell, K. ; Ray, I., "Towards a Forensic-Based Service Oriented Architecture Framework for Auditing of Cloud Logs, " Services (SERVICES), 2013 IEEE Ninth World Congress on, vol., no., pp. 75, 83, June 28 2013-July 3 2013

[6] Chenyu Zheng; Sicker, D. C., "A Survey on Biologically Inspired Algorithms for Computer Networking, " Communications Surveys & Tutorials, IEEE, vol. 15, no. 3, pp. 1160, 1191, Third Quarter 2013

[7] Wang, B. ; Li, B. ; Li, H., "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, " Cloud Computing, IEEE Transactions on, vol. PP, no. 99, pp. 1, 1

[8] Nithiavathy, R., "Data integrity and data dynamics with secure storage service in cloud, " Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on, vol., no., pp. 125, 130, 21-22 Feb. 2013

[9] Meena, S. ; Daniel, E. ; Vasanthi, N. A., "Survey on various data integrity attacks in cloud environment and the solutions, " Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on, vol., no., pp. 1076, 1081, 20-21 March 2013

[10] Sur, C. ; Shukla, A., "Dealing QAP & KSP with Green Heron optimization algorithm — A new bio-inspired meta-heuristic, " Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, vol., no., pp. 1, 8, 4-6 July 2013

[11] Rathore, H. ; Badarla, V. ; Jha, S. ; Gupta, A., "Novel approach for security in Wireless Sensor Network using bio-inspirations, " Communication Systems and Networks (COMSNETS), 2014 Sixth International Conference on, vol., no., pp. 1, 8, 6-10 Jan. 2014

[12] Fei Zhang; Yizhou Yan; Wenjun Wu; Liang Luo, "A Heuristics Approach for Reducing Power Consumption of Cloud Data Center, " Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, vol., no., pp. 246, 253, 20-23Aug. 2013.

[13] Drias, H. ; Hireche, C. ; Douib, A., "Datamining techniques and swarm intelligence for problem solving: Application to SAT, " Nature and Biologically Inspired Computing (NaBIC), 2013 World Congress on, vol., no., pp. 200, 206, 12-14Aug. 2013.

[14] Rui Tang; Fong, S. ; Xin-She Yang; Deb, S., "Wolf search algorithm with ephemeral memory, " Digital Information Management (ICDIM), 2012 Seventh International Conference on, vol., no., pp. 165, 172, 22-24 Aug. 2012