A   SURVEY PAPER ON SECURING CLOUD AND MAKING A RECORD WITHIN AN DILIGENCE

B.Sudhakar	**S Harini Yadav**	**C Praveen Kumar**
Assistant Professor	Assistant Professor	Assistant Professor
Department of computer	Department of computer	Department of computer
science and engineering	science and engineering	science and engineering
Kandula Lakshumma	Kandula Lakshumma	Kandula Lakshumma
Memorial College of	Memorial College of	Memorial College of
Engineering for Women	Engineering for Women	Engineering for Women
Kadapa,A.P	Kadapa,A.P	Kadapa,A.P

Abstract

Interestingly despite the fact that, make indistinguishable forensics is a comparatively a reduced amount of understood topic. In the event that a cloud service, cloud server, or client device has been compromised or involved in malicious cyber activity (e.g. used to host illegal contents such as radicalization equipment, or manner concentrated denial of service (DDoS) attacks) , investigators require to be able to accomplish forensic analysis in categorize to "reply the six enter questions of an unpleasant incident - could you repeat that?, why, how, who, at what time, and anywhere".

I. INTRODUCTION

The problem with such data is that we must trust the make unclear repair supplier to give us the right information. They strength give us false information or hold back some very important information. For Securing Cloud and making a Investigation A Log Management is a record of all the activities and events occurring and processed within an industry, organizations, application or system or software or network.
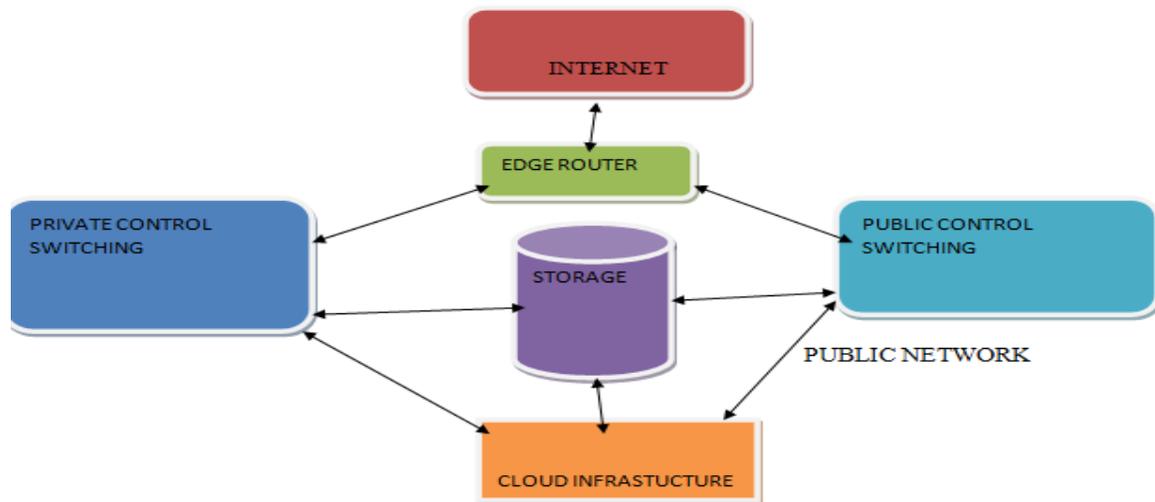

Fig:1 Secure Cloud Computing Structure

Logging of activities is important aspect because log information can be second-hand intended for decision making and troubleshooting of problems occurred at the time of working and also helps in fine tuning of system performance and identify various users who are violating policies. Project proposes an enhanced Secure Log Management for securing user activities from malicious attacks.

Log records play a significant role in digital forensic examination of systems. To maintain log security and provide protecting from attackers we design a integrated novel log security algorithm which provides security to log files at all times. As the log files contain sensitive information we require confidentiality and privacy of log records is an important.

II. IMPRESSION OF SAFETY MEASURES INSIDE CLOUD ORGANIZATIONS

Designing and deploying a secure logging Software involves significant capital expenses that many organizations may find irresistible overwhelming. Our proposed Delegating register board provides viable cost saving measure. The project identifies a novel frame work for a challenging secure cloud base log organization service. . Keywords - Watermarking, Haar Wavelet, DWT, PSNR I.

Introduction STD paper format typescript should be 10 in period new roman with single spacing.In recent years, the accessing of multimedia data or digital information has become very easy because of the fast development of the Internet. In other words, this development makes unauthorized distribution of multimedia data. For the protection of multimedia data, a solution known as watermarking is used.
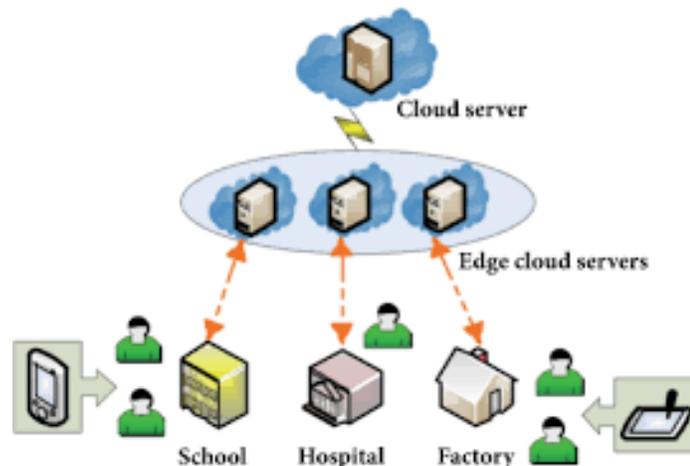

Fig:2 Secure Cloud Computing Structure in organization

After the approximate 20 years' research, different kinds of watermarking algorithm based on different theory concepts were introduced [1-3]. A digital watermark encodes the owner certify in sequence and embed it keen on data. Watermarking might be used to recognize the image

III. PROPOSED ALGORITHM

2.1 Extending SecLaaS, we propose a secure cloud logging scheme, Cloud register assure reliability and confidentiality (CLASS), designed to ensure CSP accountability (i.e.

writing the correct information to the log) and preserve the user's privacy. Specifically, we include the capability for the consumer to verify the accuracy of their log. To do this, the log will be encrypted by the user's public key (rather than the agency's public key).

To avoid introducing unnecessary delays to the forensic investigation, during user registration with the cloud service, both the CSP and the user will collectively choose a community/confidential key pair referred to as content concealing key (CC-key) for the user. The corresponding (content concealing) private key will be shared with other CSPs secret sharing schemes.
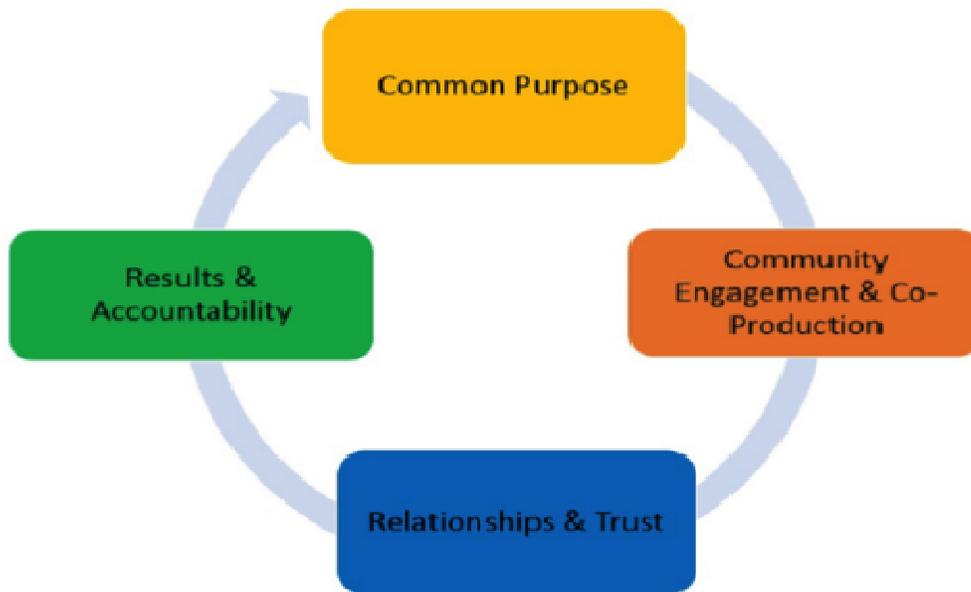

Fig:3 Effective collective impact

This would allow the private key to be regenerated whenever necessary. We also demonstrate how we can leverage Rabin's fingerprint along with bloom filter in PPL generation to establish log veracity. We then implement CLASS in Open Stack and evaluate its performance.

IV. CONCLUSION

CLASS conserve the solitude of blur users by encrypting blur firewood by means of a community key of the individual consumer at the same time as also facilitating log retrieval in the event of an investigation. Moreover, it ensures accountability of the cloud server by allowing the user to identify any log modification. This has the additional effect of preventing a user from repudiating entries in his be in possession of log once the log has had its PPL established.

Our implementation on Open Stack demonstrates the feasibility and practicality of the proposed scheme. The experimental results show an improvement in efficiency thanks to the features of the CLASS scheme, particularly in verification phase Normally logs are low-level data and hard for the common user to appreciate what exactly those logs signify.

Thus, we will explore leveraging big data techniques to facilitate user retrieval and visualization of information from log data. To ease searching, we kept some crucial and sensitive information in plaintext format. This makes them vulnerable to be exposure. Thus, designing secure and efficient searchable encryption would increase in length this occupation.

There is also the require intended for an online trustworthiness organization designed to expand faith and trustworthiness of a make unclear consumer so with the intention of the CSP can make possible stricter audit policy for low-trust users in judgment to high-trust users. ingenuous and implementing a prototype of the wished-for scheme in partnership with a real-world CSP, with the aspire of evaluate its utility (e.g. performance and scalability) in a real-world environment.

REFERENCES

[1] B. Corona, M. Nakano, H. Pérez, "Adaptive Watermarking Algorithm for Binary Image Watermarks", Lecture Notes in Computer Science, Springer, pp. 207-215, 2004. A. A. Reddy and B. N. Chatterji, "A new-fangled wavelet base logo-watermarking scheme," Pattern

[2] B. Corona, M. Nakano, H. Pérez, "Adaptive Watermarking Algorithm for Binary Image Watermarks", Lecture Notes in Computer Science, Springer, pp. 207-215, 2004. A. A. Reddy and B. N. Chatterji, "A new-fangled wavelet base logo-watermarking scheme," Pattern

[3] C Praveen Kumar, "Mining association rules from No-SQL data bases using map-reduce fuzzy association rule mining algorithm", International Journal of Applied Engineering Research, pp. 10472-10476, 2017. CP Kumar, P Anjaiah, S Patil, E Lingappa, M Rakesh - International Journal of Applied Engineering Research, 2017

[4] C Praveen Kumar "An Approach to Encore Web Pages Using User Revisitation Access based on Content Keywords"C Tejaswini, CP Kumar - International Journal of computer science Engineering ..., 2019

[5] C Praveen Kumar "An Efficient Face Recognition System Using Face Recognition Algorithms Pca, Lda And Ica"Cp Kumar, Sj Sowjanya, Rm Noorullah - International Journal Of Pure And Applied Mathematics, 2018

[6]   Reza Sheibani, Amir Ebrahimzadeh ,Member, IAUM," An Algorithm For Mining FuzzyAssociation Rules", Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I, March, 2008,pp.486-490.

[7]   K.Sangeetha,Dr.P.S.Periasamy , S.Prakash,"Efficient Parallel Pruning of Associative Rules with Optimized Search", IOSR Journal of Computer Engineering (IOSRJCE) ,volume no.3,pp.26-30.

[8] AshishMangalampalli, VikramPudi,"FPrep: Fuzzy Clustering driven Efficient Automated Preprocessing for Fuzzy Association Rule Mining", IEEE Intl Conference on Fuzzy Systems (FUZZIEEE), July 2010.

[9] G Vijay Krishna,PRadhaKrishna,"A Novel Approach for Statistical and Fuzzy association   Rule Mining on Quantiative Data ",Journal of scientific and industrial Reasearch ,vol no.67,jul2008,pp.512-517.

[10] Chang et al., 2009, Chang E.Y., Bai H., and Zhu K., Parallel algorithms for mining large-scale richmedia data, In: Proceedings of the 17th ACM International Conference on Multimedia (MM '09), New York, NY, USA, 2009, pp. 917-918.

[11] Chen et al. 2004, R. Chen, K. Sivakumar, and H. Kargupta, Collective Mining of Bayesian Networks from Distributed Heterogeneous Data, Knowledge and Information Systems, 6(2):164-187, 2004.

[12] Chen et al. 2012, Yi-Cheng Chen, Wen-Chih Peng, Suh-Yin Lee, Efficient algorithms for influence maximization in social networks, Knowledge and Information Systems, December 2012, Volume 33, Issue 3, pp 577-601

[13] Chu et al., 2006, Chu C.T., Kim S.K., Lin Y.A., Yu Y., Bradski G.R., Ng A.Y., Olukotun K., Mapreduce for machine learning on multicore, In: Proceedings of the 20th Annual Conference on Neural Information Processing Systems (NIPS '06), MIT Press, 2006, pp. 281-288.

[14] Cormode G. and Srivastava D. 2009, Anonymized Data: Generation, Models, Usage, in Proc. Of SIGMOD, 2009. pp. 1015-1018.

[15] Das et al., 2010, Das S., Sismanis Y., Beyer K.S., Gemulla R., Haas P.J., McPherson J., Ricardo: Integrating R and Hadoop, In: Proceedings of the 2010 ACM SIGMOD International Conference on Management of data (SIGMOD '10), 2010, pp. 987- 998.

[16] Dewdney P., Hall P., Schilizzi R., and Lazio J. 2009, The square kilometre Array, Proc. of IEEE, vol.97, no.8.

[17] Domingos and Hulten, 2000, Domingos P. and Hulten G., Mining high-speed data streams, In: Proceedings of the sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD00), 2000, pp. 71-80.

[18] Duncan G. 2007, Privacy by design, Science, vol. 317, pp.1178-1179. 20) Efron B. 1994,   Missing data, imputation, and the Bootstrap, Journal of the American Statistical Association,   vol.89, no.426, pp.463-475.