International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Public Auditing for Secure Cloud Storage using MD5 Algorithm

A. Viji Amutha Mary, Mercy Paul Selvan, Christy

Abstract— Cloud computing has become a significant technology trend, and plenty of consultants expect that cloud computing can reshape data technology (IT) and also the IT marketplace. In this paper, we are suggesting a safety mechanism that provides open analysis on shared knowledge within the cloud. During this mechanism, the individual of the underwriter on every sq. in shared statistics are going to be hold on in private from open verifies, who can proficiently verify the shared records without improving the entire report. This mechanism can play out numerous comparing undertakings at the identical time instead of checking them separately. This framework provides a security saving options of open inspecting part for shared facts at intervals the cloud. we have a tendency to area unit mistreatment ring marks to make homomorphy authentication, so thereto, AN open verify will offer an summary on shared data while not obtaining the entire facts, but it cannot be understanding that who is the underwriter on every piece. To get the effectiveness of confirming numerous examining undertakings, we facilitate to increase our tool for better examining. Certainly, the tractability implies the capacity to gather administrator to find the person of the underwriter in the metadata of few great instances.

Keywords : Privacy Preserving, Public Auditing, TPA, Security

I. INTRODUCTION

The clients concern about data security, data integrity, and data sharing data must be addressed. The challenges can be overcome by encryption of data and storing the same to the cloud server. Hash computation can be performed and the hash data can be cached in the client machine. It is very confidential to store and share the data in the client side. It becomes a security threat if such stored data is vulnerable to attack. So an alternative method has to be found out to log the data in the cloud in an efficient and safety way.

Manuscript published on 30 September 2019
* Correspondence Author
A. Viji Amutha Mary *, Associate Professor, Dept of CSE, Sathyabama Institute of Science and Technology, Chennai-119, vijiamumar@gmail.com
Mercy Paul Selvan, Assistant Professor, Dept of CSE, Sathyabama Institute of Science and Technology, Chennai-119, mercypaulselvan@gmail.com
Christy, Professor, Dept of CSE, Sathyabama Institute of Science and Technology, Chennai-119, christy.cse@sathyabama.ac.in

II. LITERATURE SURVEY

The cloud framework is isolated into two spaces – open area and individual area. A productive key administration framework for individual wellbeing record was kept up in the cloud[1]. A protection safeguarding open inspecting framework for information stockpiling security in Cloud Computing was recommended in 2013[2]. Homomorphism direct authenticator and arbitrary veiling approach was used to ensure that the TPA would not rely upon the put away information on the cloud server. The significant drawback is that the individual evaluating of these developing undertakings can be monotonous and lumbering. Effective and Secure Multi-Watchword Search on Encoded Cloud Information was actualized on 2012 [3]. The calculation and correspondence expenses of this strategy are very huge since each search term in a question requires a few homomorphism encryption activities both on the server and the client side. In Oruta, TPA can productively review the honesty of shared information, yet can't recognize who is the underwriter on each square, which can protect character security for clients [4]. The data is classified to the gathering and ought not be uncovered to any outsider. Panda, An open examining for Imparted Information to Productive Client Renouncement in the Cloud was proposed in 2013 [5]. At the point when a client in the gathering is disavowed, semi-believed cloud is permitted to re-sign obstructs that were marked by the repudiated client with intermediary re-marks. The client can't access and alter shared information. Information honesty can be confirmed with just the open keys of existing clients. In Dec 2013, shared information was put away on the cloud by means of Security-Middle person [6]. The data is private to the gathering and ought not be uncovered to any outsider. Open examining for guaranteeing cloud information stockpiling security with zero learning Protection was presented in the year 2009 [7]. A Protected Model for Cloud Information Stockpiling was proposed in the year 2012 [8]. Each Model has its very own upsides and downsides. Open Auditability and Information Elements were empowered for Capacity Security in Distributed computing in the year 2011.

III. SYSTEM ARCHITECTURE

The system architecture of the public auditing system is depicted in Fig 1. A mechanism which checks the data integrity and which saves the computation resources of the cloud users is public auditing. The examining component is finished by TPA, outsider reviewer. TPA confirms the rightness of the cloud information on interest without recovering a duplicate of the entire information.

TPA has ability and capacities that can occasionally check the honesty of the considerable number of information put away which gives a simpler and reasonable path for the clients to guarantee their capacity accuracy in the cloud.

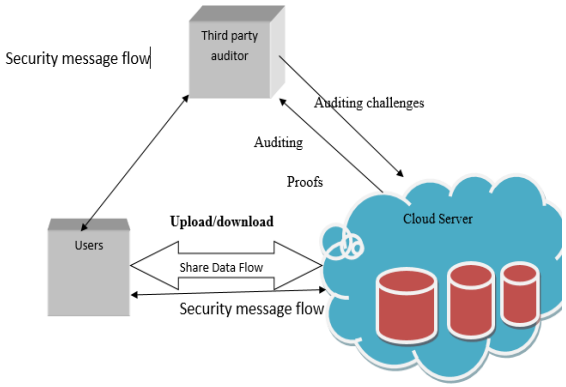

Fig 1. System Architecture

IV. PROPOSED SYSTEM

The proposed framework gives a protection saving open reviewing component for shared information in the cloud. We use ring marks to build homomorphism authenticators, so an open verifier can review shared information trustworthiness without recovering the whole information, yet it can't recognize who is the underwriter on each square. Performance is improved by extending the support to batch auditing. The interesting problem to be worked with the future is recognizability, which means the capacity for the group head to uncover the character of the underwriter dependent on metadata in some uncommon circumstances.

Advantages of proposed system

- The proposed framework can play out various examining undertakings at the same time
- They improve the effectiveness of verification for different evaluating undertakings.
- High security will be accommodated for sharing records.

V. RESULTS AND DISCUSSIONS

Fig 2 clarifies client enlistment process with character and the gathering supervisor haphazardly chooses a number. After enlistment, client gets a private key which is utilized for creating bunch signature and for unscrambling the document.

Fig 3 is for making bunch individuals with benefits for keeping up put away information under Information Proprietors gathering. The authoritative application is information sharing. The open evaluating property is particularly helpful when we anticipate that the designation should be proficient and adaptable. The plans empower a substance supplier to share her information in a secret and specific way, with a fixed and little figure content development, by dispersing a solitary and little total key to each approved client.

Fig 4 and Fig 5 demonstrate the procedure of Homomorphic authenticators check of metadata created from individual information squares, which can be safely amassed in such a manner to guarantee an evaluator that a straight mix of information squares is accurately registered by confirming just the totaled authenticator. A way to deal with incorporate Homomorphic authenticator with arbitrary cover system is proposed. A straight mix of inspected hinders in the server's reaction is veiled with irregularity created by a pseudo arbitrary capacity (PRF).

VI. CONCLUSION

The proposed framework gives a security safeguarding open inspecting component for shared information in the cloud. Ring marks are used to develop homomorphism authenticators, so an open verifier can review shared information trustworthiness without recovering the whole information, yet it can't recognize who is the underwriter on each square. The customer can share the information safely with explicit band of individuals with no overhead of key circulation.

Retrieval Number: B1929078219/2019©BEIESP
DOI:10.35940/ijrte.B1929.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

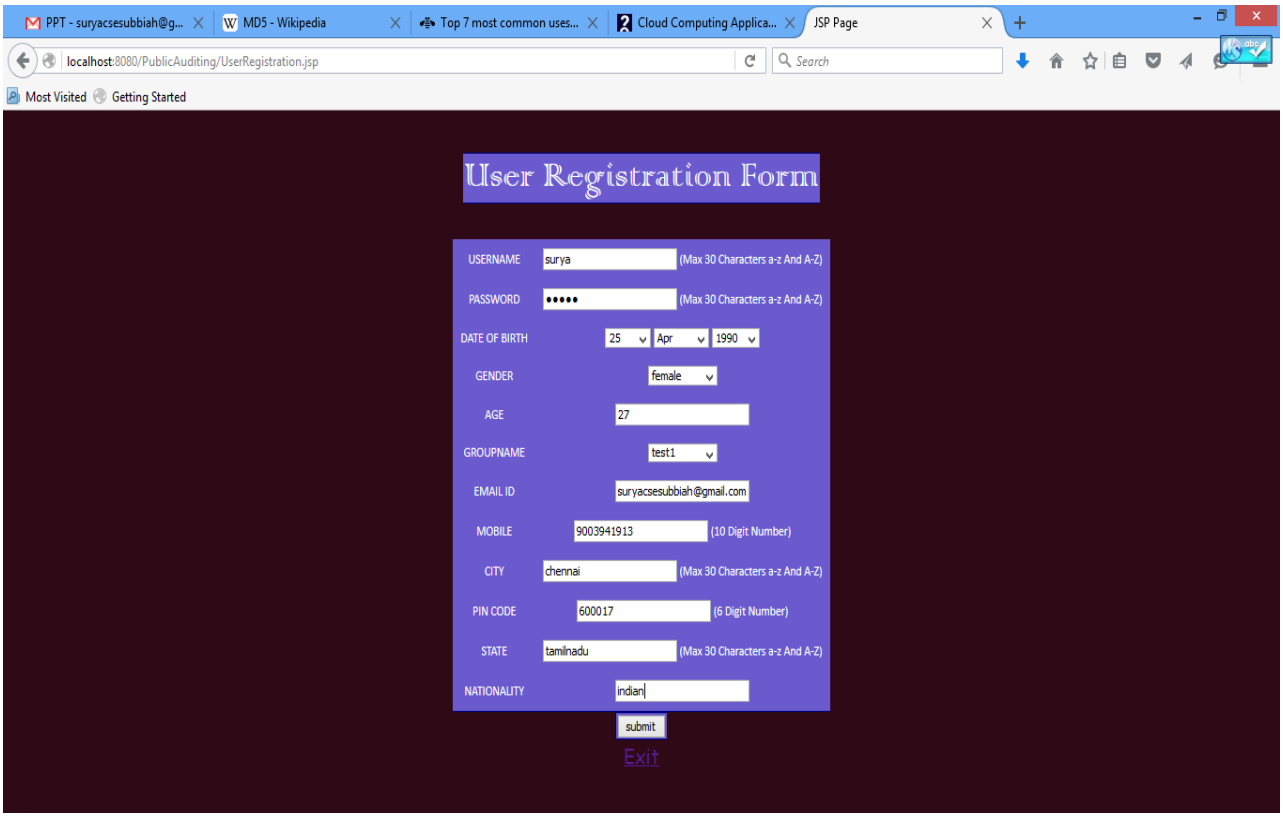

Fig 2 User Registration Screen

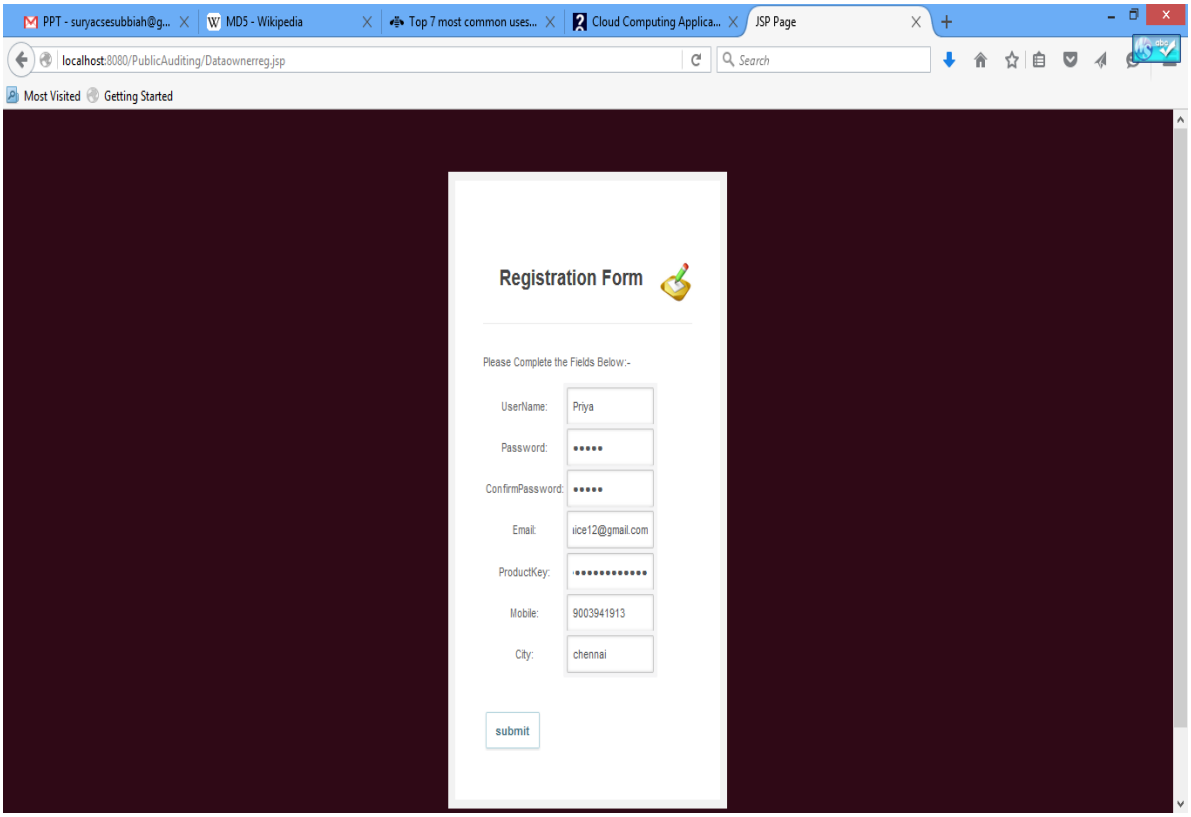

Fig 3 Data Owner Registration

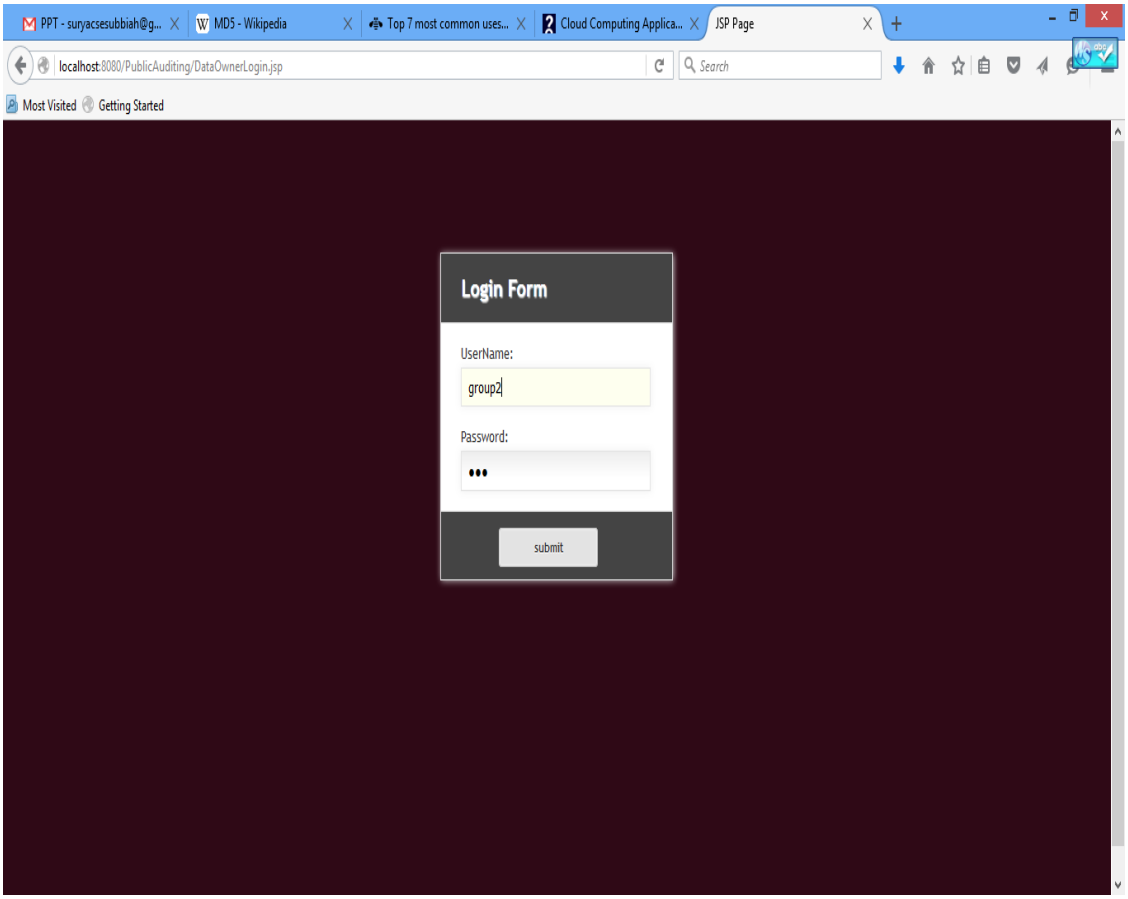

Fig 4 Data Owner Login

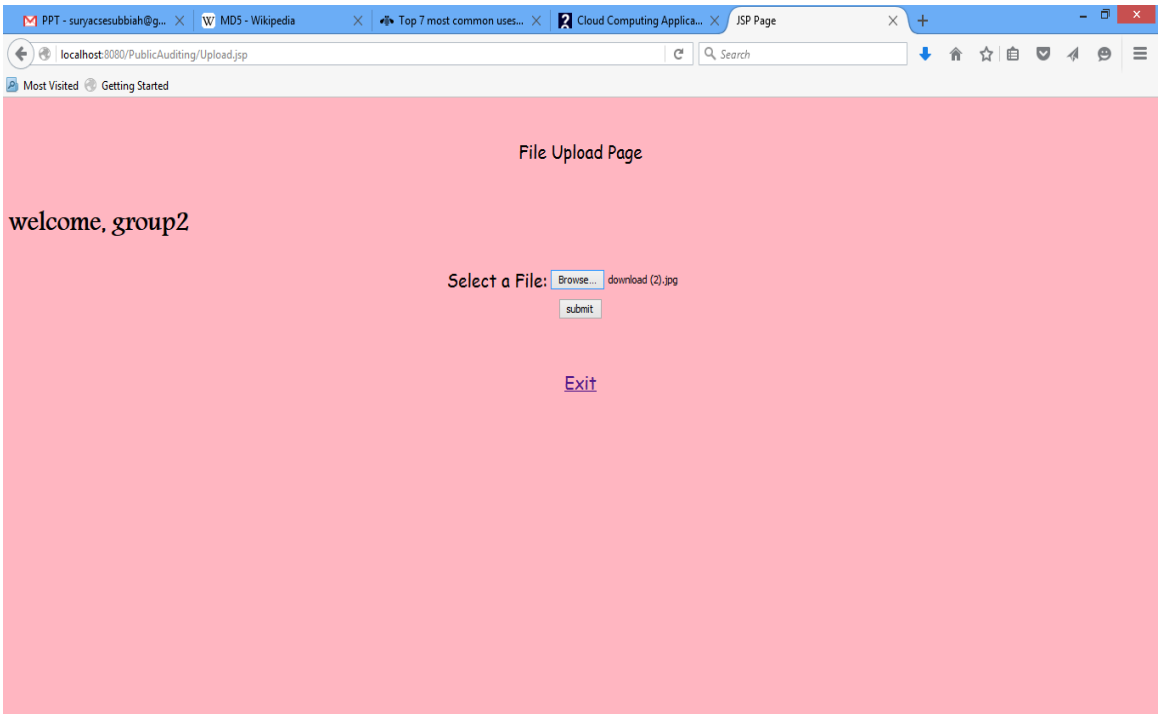

Fig 5 File Upload Screen

REFERENCES

1. Franjoe Morais B, JayaChandar, and Viji Amutha Mary A, "An Efficient Key Management Infrastructure for Personal Health Record in Cloud", Research Journal of Pharmaceutical, Biological and Chemical Sciences, Vol 8, No 2, March- April 2017.
2. C Wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage",IEEE Trasaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.
3. Y. Prasanna, Ramesh, "Efficient and Secure Multi Keyword Search on Encrypted Cloud Data", IJCST Vol. 3, Issue 3, July - Sept 2012.
4. Boyang Wang , Baochun Li and Hui Li "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", State Key Laboratory of Integrated Services Networks, Vol 13, January 2014.
5. Boyang Wang and Baochun Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE, Vol 20 December 2013.
6. Boyang Wang, Sherman S. M. Chow, Ming Li, and Hui Li, "Storing Shared Data on the Cloud via Security-Mediator" State Key Laboratory of Integrated Service Networks, Vol 12, December 2013
7. Wang Shao-hu, Chen Dan-we, Wang Zhi-weiP, Chang Su-qin, "Public auditing for ensuring cloud data storage security with zero knowledge Privacy" College of Computer, Nanjing University of Posts and Telecommunications, China, 2009
8. KunalSuthar, Parmalik Kumar, Hitesh Gupta, "SMDS: Secure Model for Cloud Data Storage", International Journal of Computer applications, Vol 56, No.3, October 2012
9. Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transaction on Parallel and Distributed System, vol. 22, no. 5, pp. 847 – 859, 2011.

AUTHORS PROFILE

A. Viji Amutha Mary was born on 1st August 1981 at Aruppukottai, India. Her native is Tirunelveli, India. She did her schooling in Tuticorin and Tirunelveli. She completed her Bachelor of Engineering degree in Computer Science and Engineering discipline in the year 2003 from Manonmaniam Sundaranar University, Tamil Nadu. She completed her Master degree in Computer and Information Technology in the year 2005 from the same University. In the same year, she joined as a Lecturer in Sathyabama University, Chennai and currently she is working as an Associate Professor in the Department of Computer Science and Engineering. Her total teaching experience counts to fourteen years. She was awarded Doctorate degree in the year 2018 in Computer Science and Engineering. Her research interests include Data Mining and Image Processing. She has published around 30 journals.

Mercy Paul Selvan was born on 18th April 1976 at Chennai, Tamil Nadu. She received her Bachelor of Science in Computer Science from Madras University and Master of Science in Information Technology from Annamalai University. She got her Master degree in Computer Science & Engineering from St. Joseph's College of Engineering, Jeppiar Nagar, Sholinganallur, Chennai, Tamil Nadu. She pursued Doctorate Degree in Computer Science Engineering in the field of Web Mining. She is currently working as Assistant Professor in Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India. Her area of interest in research includes Data Mining, Machine Learning, Big Data, Data Science, Distributed Systems etc. She has ten years of teaching experience. She published more than 25 papers in various reputed journals and conferences. She had guided more than 30 undergraduate and postgraduate student projects till date.

Christy A. is working as Professor in the Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai. She has done her research in the area of Text Mining with the title Integration of Information Extraction with Machine Learning Techniques for Text Mining. Her research interests include Text Mining, Data mining. She is also interested in the areas of Machine Learning, Big Data Analytics, Artificial Intelligence, Genetic Computing, Remote Sensing, Spatial Data Analysis and Data Security. She has published many papers in International Journals/ National Journals and Proceedings. She has also participated and presented papers in International and National Conference.