International Journal of Computer Science Trends and Technology (IJCST) – Volume 10 Issue 5, Sep-Oct 2022

RESEARCH ARTICLE OPEN ACCESS

Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments

MR D. Purushothaman MCA., M.E. [1], K Priya Dharshini [2]

[1] Asst. Professor, Department of Computer Applications
[2] Student, Department of Computer Applications
[1],[2] Chadalawada Ramanamma Engineering College

ABSTRACT

With the maturity of cloud computing technology in terms of reliability and efficiency, a large number of services have migrated to the cloud platform. To convenient access to the services and protect the privacy of communication in the public network, three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server architectures gain wide attention. However, most of the existing three-factor MAKA protocols don't provide a formal security proof resulting in various attacks on the related protocols, or they have high computation and communication costs. And most of the three-factor MAKA protocols haven't a dynamic revocation mechanism, which leads to malicious users can not be promptly revoked. To address these drawbacks, propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management using Schnorr signatures and provides a formal security proof in the random oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. Performance analysis demonstrates that the proposed scheme is well suited for computing resources.

Keywords: - Cloud computing, protocols, Mutual Authentication, Key Agreement.

I. INTRODUCTION

Performance analysis demonstrates that the proposed scheme is well suited for computing resource constrained smart devices. The full version of the simulation implementation proves the feasibility of the protocol. the system proposed a key management system for hybrid servers, which aims to compute personalized trust results based on the similarity of two users when making choices which leads less security. propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management using Schnorr signatures and provides a formal security proof in the random oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. In 2001,introduced the concept of authentication protocol for multi-server environments and proposed the first password-based MAKA protocol using the neural network.

Thanks to the complicated neural network, Li et al.'s protocol isn't suitable for smart devices with limited computing power.

To improve efficiency, author proposed a MAKA protocol for multi-server architectures by using hash functions and symmetric key cryptosystems. In the same year, Chang et al. pointed out that Juang's protocol is flawed in terms of efficiency. They proposed a more efficient MAKA scheme for multi-server environments. However, in their protocol RC shares system private key with all servers. In the existing work, the system proposed a key management system for hybrid servers, which aims to compute personalized trust results based on the similarity of two users when making choices which leads less security. The existing scheme leaks the existing trust relationships between users of the same CSP. And it cannot compute customized evaluation results and ensure user anonymity lack of strong finger print authentication.

II. RELATEDWORKS

W Lou and Y T Hou proposed Identity-Based Auditing for Shared Cloud Data With Efficient and Secure Sensitive Information Hiding**.** The advent of cloud computing arouses the flourish of data sharing, promoting the development of research, especially in the fields of data analysis, artificial intelligence, etc. In order to address sensitive information hiding, auditing shared data efficiently and malicious manager preventing, propose an identity-based auditing scheme for shared cloud data with a secure mechanism to hide sensitive information. Y Lang and W Young proposed Location-Based Optimized Service Selection for Data Management with Cloud Computing in Smart Grids. To maximize the utilization, reliability and availability of power resources, some distribution strategy has to be implemented, which is possible

nowadays with the support of modern information technologies (IT). To further develop power utilization, the customer should be aware of efficient power utilization, and the problem of customer management has to be resolved, where payment of electric bills could be through online solutions.

III. PROPOSED SYSTEM ARCHITECTURE

The system designs a three-factor MAKA protocol which implements three-factor security. And show that the proposed protocol can meet the demands of multi-server architectures such as anonymity, nontraceability, resistance password guessing attack and smart card extraction attack, and so on. This scheme achieves the user's dynamic management. In our protocol, users can be dynamically revoked to promptly prevent attacks from malicious users. Without a dynamic revocation mechanism, RC can't punish malicious users in a timely manner. This may result in such malicious users still active in the network to communicate with other servers. In the random oracle, provide a formal proof of the proposed protocol based on BDH, CDH and Schnorr signatures unforgeability assumptions. show that the proposed protocol is mutual authentication secure and authenticated key agreement secure. Our protocol has a good execution efficiency. Especially on the client side, the computation cost of our scheme is the lowest in the related existing protocols. This shows that our protocol is more suitable for device mobiles with limited computing resource. And, to prove that the protocol is technically sound, we programmatically simulate the proposed protocol. The system is more effective since three-factor Mutual Authentication and Key Agreement is used. The system is more secured since the secret sharing network can be formed by the users/raters to protect their data privacy.

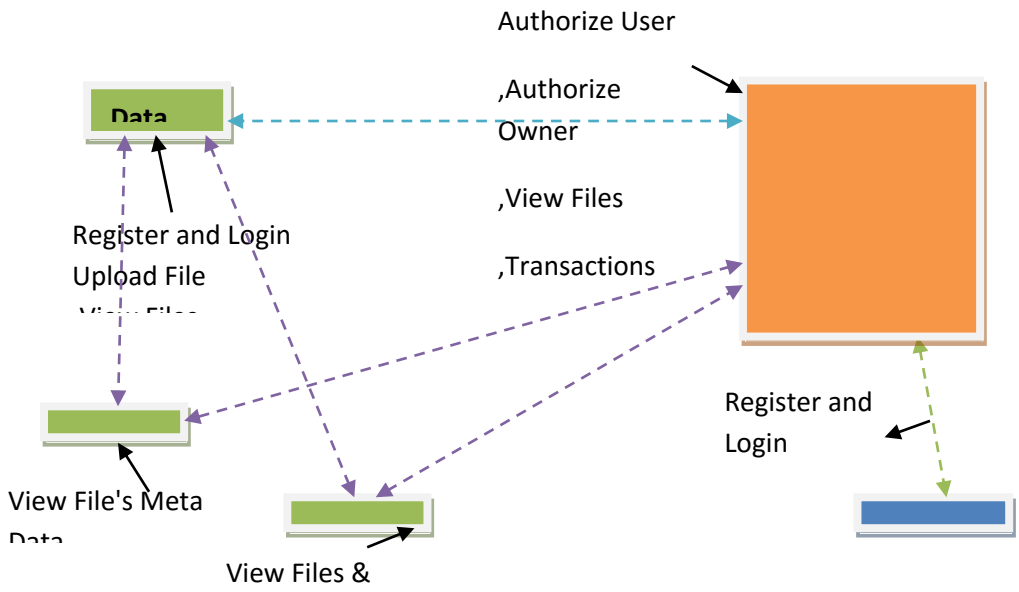

Fig.1 Proposed system architecture

Data Owner: The following are the functionalities provided by the Data Owner:

- login
- Upload Files
- View files
- Update files
- Verify files block
- Log out

End User: The following are the functionalities provided by the End User:

- Register & Login
- Search
- Download
- View files
- Search request

- Download request
- Log Out

Cloud Server: The following are the functionalities provided by the Cloud Server:

- Login
- Authorize user
- Authorize owner
- View files
- Transactions
- Search request
- Download request
- View Attackers
- View file rank in chart
- View time delay results
- View through put results
- Log Out

TPA: The following are the functionalities provided by the TPA:

- Login
- View files meta data
- CPU Speed
- Log out

KGC: The following are the functionalities provided by the KGC:

- Login
- View file & Generate secret key
- Logout

IV. RESULTS AND DISCUSSION

The output screens obtained after running and executing the system are shown from Fig.2 to Fig.8

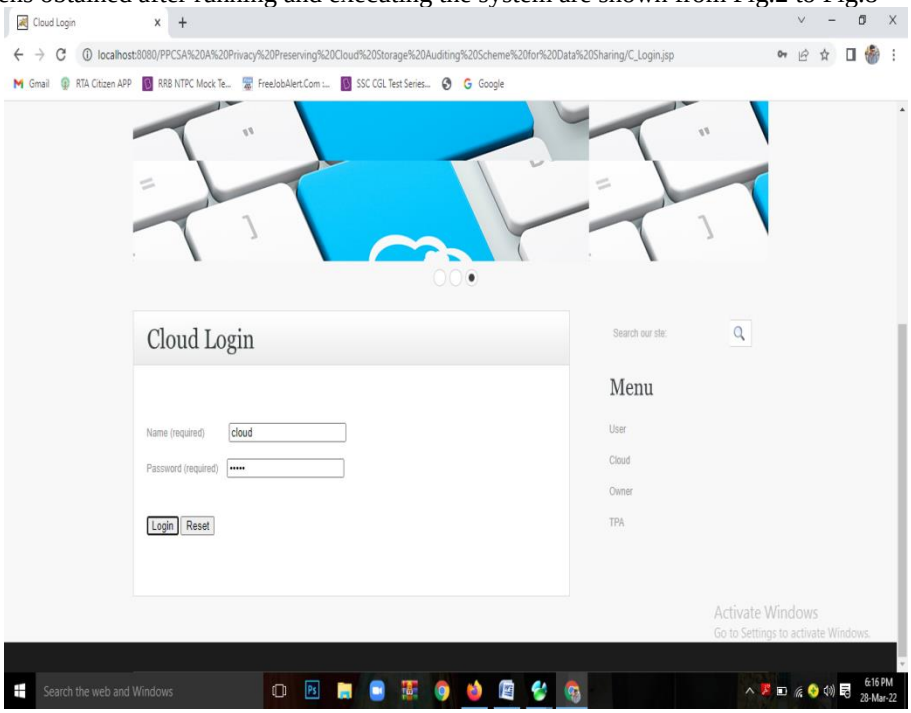

Fig.2 Cloud Login

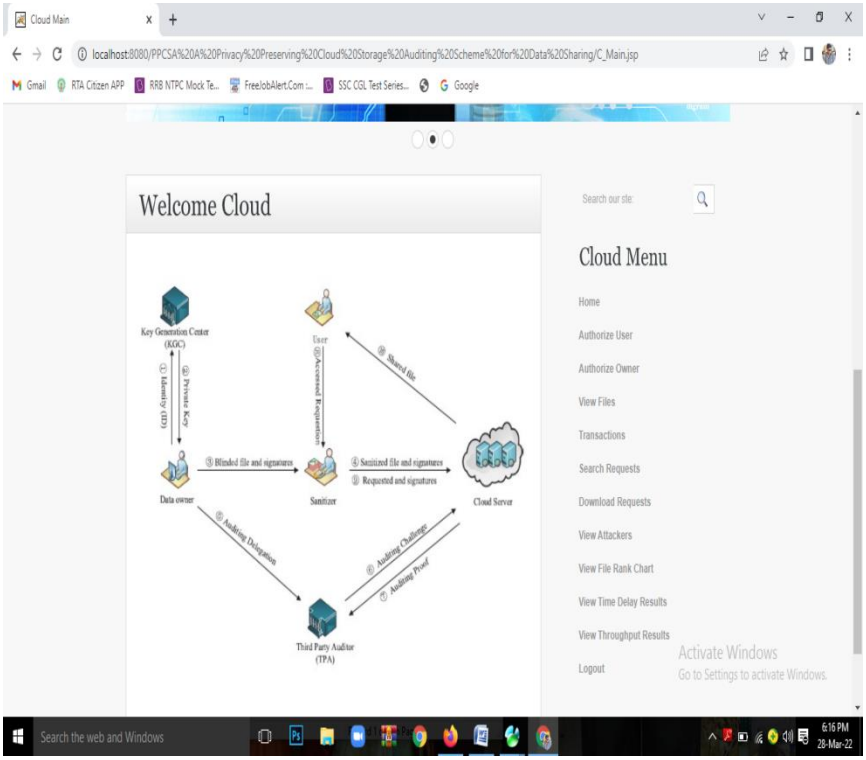

Fig.3 Cloud Home page

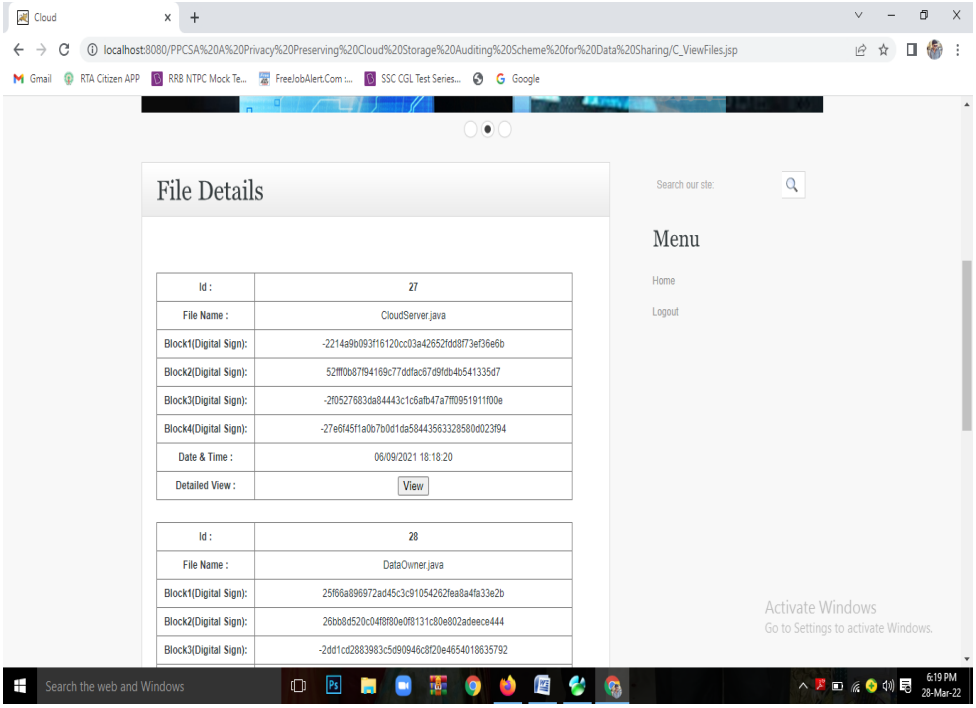

Fig.4 File Details

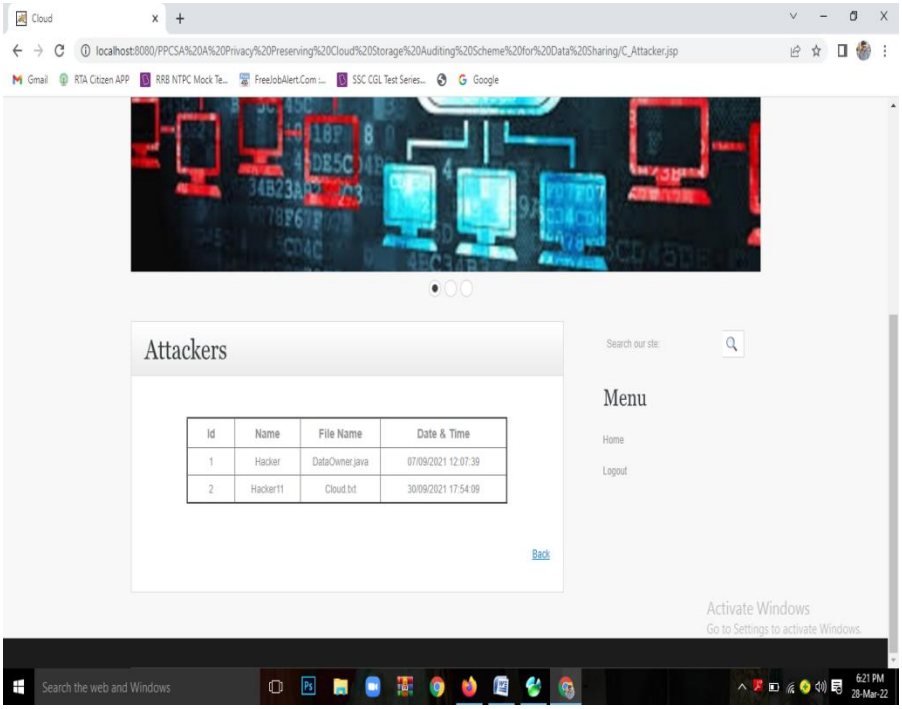

Fig.5 Attackers

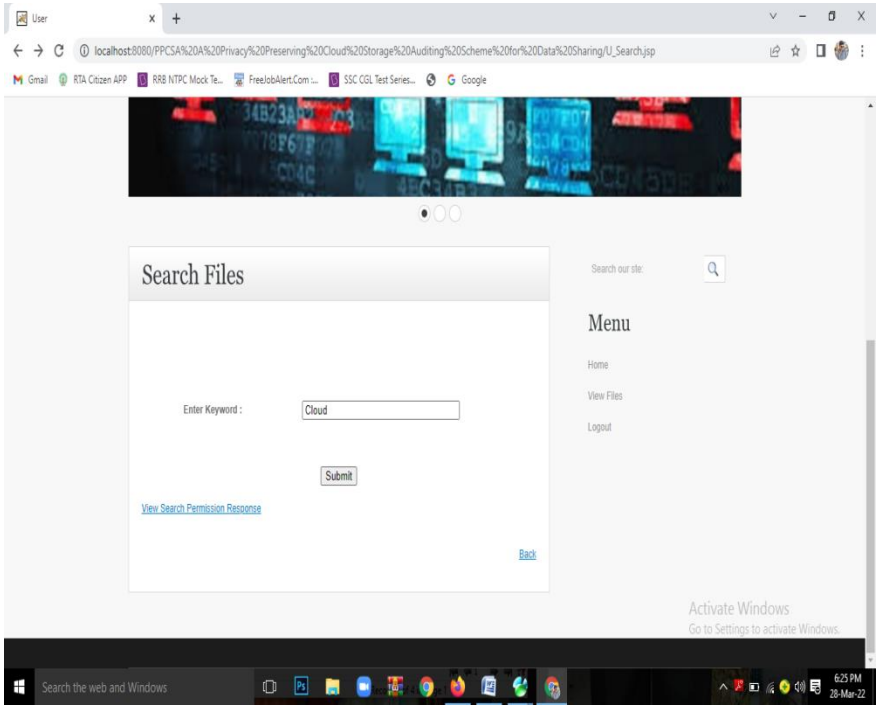

Fig.6 search Files

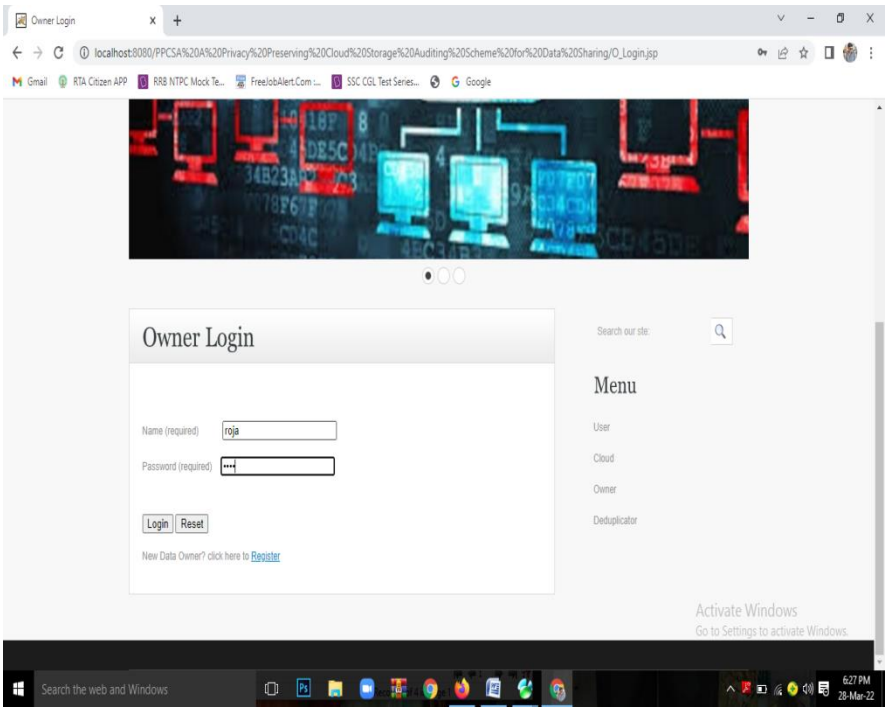

Fig.7 Owner Login

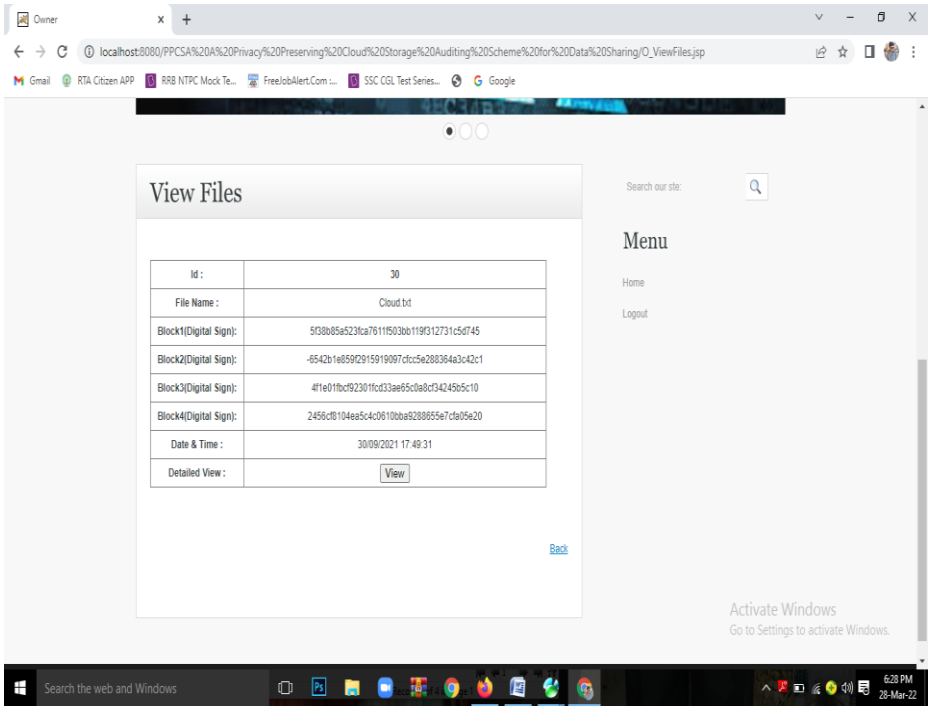

Fig.8 View Files

V. FUTURE SCOPE AND CONCLUSION

Most of the three-factor MAKA protocols haven't a dynamic revocation mechanism, which leads to malicious users can not be promptly revoked. To address these drawbacks, propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management using Schnorr signatures and provides a formal security proof. Security analysis shows that our protocol can meet various demands in the multi-server environments.

REFERENCES

[1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing,” Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index. html, 2009.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[3] M. Arrington, “Gmail disaster: Reports of mass email deletions,” Online at http://www.techcrunch.com/2006/ 12/28/gmail-disasterreports-of-mass-email-deletions/, December 2006.

[4] J. Kincaid, “MediaMax/TheLinkup Closes Its Doors,” Online at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[5] Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[6] Satish, Karuturi S R V, and M Swamy Das. "Quantum Leap in Cluster Efficiency by Analyzing Cost-Benefits in Cloud Computing." In Computer Science and Engineering by Auroras Scientific Technological & Research Academy Hyderabad, vol. 17, no. 2, pp. 58-71. Accessed 2018.