Protocol design for secure authentication of keys in cloud computing

Mrs.T.Sruthi [1], Harsh Jaiswal (20S11A1216) [2], Debabandya Chaini (20S11A1211) [3], K.Manoj Kumar (20S11A1220) [4], Soujanya Manne (20S11A1240) [5],

ASSISTANT PROFESSOR [1], UG STUDENTS [2,3,4,5,]

DEPARTMENT OF INFORMATION TECHNOLOGY

MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE,

Maisammaguda, Medchal (M), Hyderabad-500100, T. S

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 cannot be promptly revoked. To address these drawbacks, we 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 resource constrained smart devices. The full version of the simulation implementation proves the feasibility of the protocol.

INTRODUCTION

In this century where the majority of people are aware of technology and how it works, many of them indulge in unlawful activities. One of such activities is the production of fake currency which is practiced to deceive people. In this proposal, it is focused on this illegitimate practice and try to bring forward a solution for it. According to a survey, the maximum number of cases of counterfeit in India still relate to fake currency, There were 132 cases of counterfeit currency in 2018, which shot up 37 percent to 181 in 2019. In Order to stop this fraudulent activity, a system is proposed that can be integrated into electronic devices that will detect the fake note as soon as it is scanned by the device. Some of the techniques which are considered are used previously and include KNN which will be utilized in the proposed system with enhanced accuracy. K-nearest neighbour's (KNN) is an algorithm that stores all the available data and classifies a new data point based on the similarity. This means when new data appears then it can be easily classified into a good suite category by using the KNN algorithm. Usually, the Euclidean distance is used as the distance metric. Then, it assigns the point to the class among its k nearest neighbour's (where k is an integer). As k-NN does not require the off- line training stage, its main computation is the on-line 'searching' for the k nearest neighbours of a given testing example. Although using different k values are likely to produce different classification results, 1-NN is usually used as a benchmark for the other classifiers since it can provide reasonable classification performances in many pattern classification problems.

LITERATURE SURVEY

The first survey of detecting site visitors from social media as

[1] Zhen-Yu Wu dialect, et. al., presents the survey paper A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network Publisher at 2012. Protocols of user authentication square measure able to make sure the security of information transmission and users' communication over insecure networks. Among varied documented mechanisms run presently, the password-based user authentication, owing to its potency, is that the most generally used in several areas, like laptop networks, wireless networks, remote login, operation systems, and direction systems. as it is blessed with the property of straightforward and human unforgettable, that causes such associate degree attack of brute force, for instance, the previous works typically suffer off-line password shot attack. Therefore, associate degree meliorative password-based authentication theme is projected during this paper, achieving to resist off-line

password shot attacks, replay attacks, on-line password shot attacks, and ID-theft attacks. In lightweight of security, the projected theme is given sensible utility, even over insecure network.

[2] Xinyi Huang, et. al., presents the survey paper of Robust Multi-Factor Authentication for Fragile Communications at 2014. In large-scale systems, user authentication sometimes needs the assistance from the central authentication server via networks. The authentication service might be down or unavailable to natural disasters or various cyber-attacks on communication channels. This has raised serious considerations in systems which require sturdy authentication in emergency things. The contribution of this paper is two-fold. During a slow affiliation scenario, we have a tendency to gift a secure generic multi-factor authentication protocol to hurry up the complete authentication method. Compared with another generic protocol within the literature, the new proposal provides an equivalent perform with vital enhancements in computation and communication. Another authentication mechanism, that we have a tendency to name complete authentication, will manifest users once the affiliation to the central server is down. We have a tendency to investigate many problems in complete authentication and show how to add it on multi-factor authentication protocols in an economical and generic way.

[3] Chin-Chen Chang, et. al., presents the survey paper of an efficient multi-server password authenticated key agreement scheme using smart cards with access control. Due to the speedy development of science and techniques, users will remotely access computers over the networks. Thus, user authentication and key agreement become additional and additional vital to confirm the lawfulness of the user and also the security of later communications, severally. as a result of the amount of servers providing the facilities for the user is sometimes over one, the idea of multi-server protocols is introduced. On the web, every server sometimes provides varied services, and every service provided by the server might not be accessed by the user. Hence, access management is needed within the multi-service atmosphere. In 2004, Juang planned a multi-server authentication scheme with key agreement. However, access management isn't taken under consideration in Juang's planned scheme, therefore we have a tendency to propose. An economical multi-server password authentication key agreement theme with access management during this article.

[4] Chu-Hsing Lin, et al., presents the survey paper of On the security of ID-based password authentication scheme using smart cards and fingerprints at 2005. This paper proposes the algorithm of two id based password authentication schemes where there is no need of passwords or verification tables such as smart card and fingerprint. With this schemes, user can easily change their passwords. The proposed nonce based authentication scheme can withstand the occurrence of message replay attacks for a network without synchronization clocks. These schemes require each user's knowledge, possession and biometrics for each user authentication and this feature makes our scheme more reliable.

Existing system

Earlier MAKA protocols are designed for single-server architecture. As Internet users grow exponentially, the number of cloud servers rendering different services has also grown significantly. For the single-server architecture, it is difficult for users to maintain a variety of passwords for each server. To improve user experience, many scholars propose more flexible MAKA protocols for multi-server environments. Combined with the unified management features of the cloud platform, such protocols can be conveniently applied. users and cloud servers only need to register in the registration center (RC) to mutual authentication and key agreement.

Disadvantages of Existing System

In the multi-server environments, the MAKA protocols can be further divided into two categories, two-factor MAKA protocols, namely identity, password, and three-factor MAKA protocols, namely identity, password, biometrics. The works in [11], [12] have shown that the password- based MAKA protocols suffer from several attacks such as guessing password attack.

Proposed System

We propose a dynamic revocable three-factor mutual authentication and key agreement (3DRMAKA) protocol which has more comprehensive functions, reliable security and relatively higher execution efficiency. Our contribution can be summarized as follows: We design a three-factor MAKA protocol which implements three-factor security. And we 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. Our

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, we provide a formal proof of the proposed protocol based on BDH, CDH and Schnorr signatures unforgeability assumptions. We show that the proposed protocol is mutual authentication secure and authenticated key agreement secure. 4) 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.

Advantages of Proposed System

Proposed a biometrics based MAKA protocol for multi-server environments. Unfortunately, after our analysis in the security comparisons and cryptanalysis subsection of this paper, their protocol is vulnerable the server impersonation attack and the man-in the-middle attack. On the other hand, the MAKA protocol is also widely used in other environments, such as Passive Internet of Things.

SYSTEM DESIGN

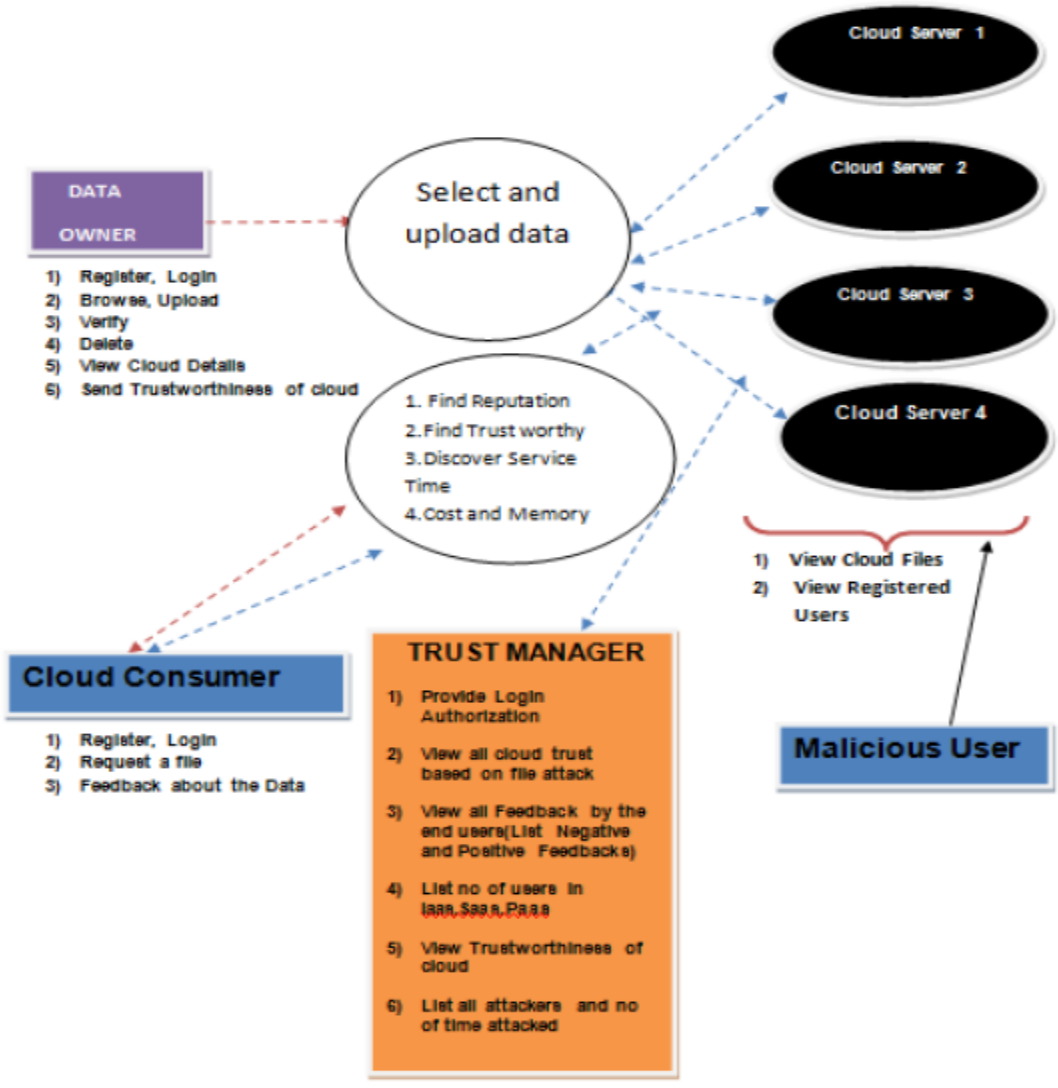

Figure 1 Block Diagram

Hardware Requirements

Processor	-	Intel Core i5-13600KF
RAM	-	16 GB (min)
Hard Disk	-	40 GB(Min)
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

Software Requirements

Operating System	-	Windows 11
Coding Language	-	Java/J2EE(JSP,Servlet)
Front End	-	J2EE
Back End	-	MySQL

INPUT AND OUTPUT DESIGN

INPUT DESIGN:

The input design for a machine learning system for fake currency detection is a fundamental aspect of building an effective model. To create a robust and accurate detection system, it is essential to start with a dataset of high-quality banknote images, encompassing both genuine and counterfeit examples. Preprocessing these images is a critical initial step, involving operations such as resizing, cropping, and noise reduction to ensure standardization. Feature extraction is then employed to capture relevant information from the images. Features can be categorized into visual, security, geometric, and ink-related characteristics. Data augmentation techniques should be used to introduce variations and enhance model robustness. Following this, the dataset should be meticulously labeled, and a balanced representation of both genuine and counterfeit banknotes should be ensured. Features should be normalized, standardized, and possibly reduced in dimensionality, and labels encoded for machine learning compatibility. The dataset can then be split into training, validation, and testing sets. Careful selection of the machine learning model, scaling, regularization, and hyper parameter tuning are essential steps.

OUTPUT DESIGN:

The output design for a machine learning system for fake currency detection is a crucial component that defines how the model's findings are communicated and utilized. Once the model processes input data, it must provide clear and actionable results. In the context of fake currency detection, the output is typically a binary classification that identifies a banknote as either genuine or counterfeit. To ensure the usability of the output, it is essential to convey not only the classification but also a confidence score or probability associated with the decision. This can help end-users make informed choices, particularly in scenarios where there may be uncertainty. Furthermore, the output design should ideally include visual feedback, highlighting the areas or features contributing to the classification decision. Finally, the output should be easily integrated into the specific application, such as a financial transaction system, an ATM, or a currency sorting machine, so that immediate actions can be taken based on the model's findings. The goal of output design in fake currency detection is to provide accurate, interpretable, and actionable results to enhance security and mitigate the circulation.

Test Results:

All the test cases mentioned above passed successfully. No defects encountered.

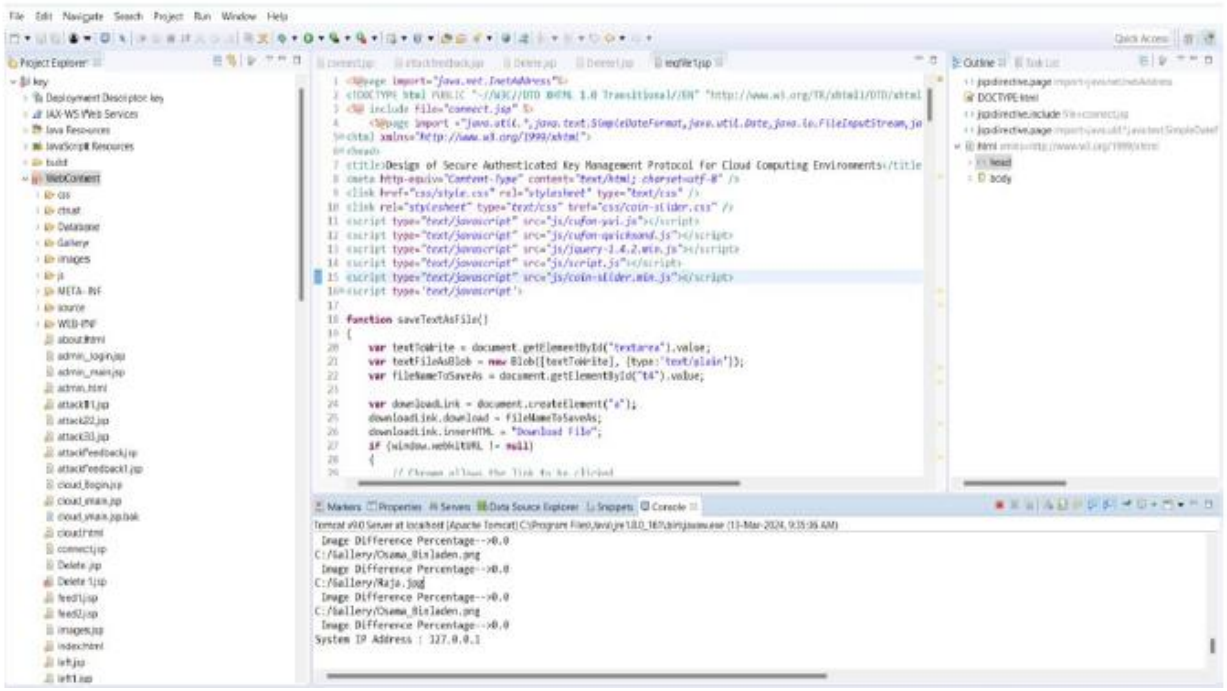

Figure 2

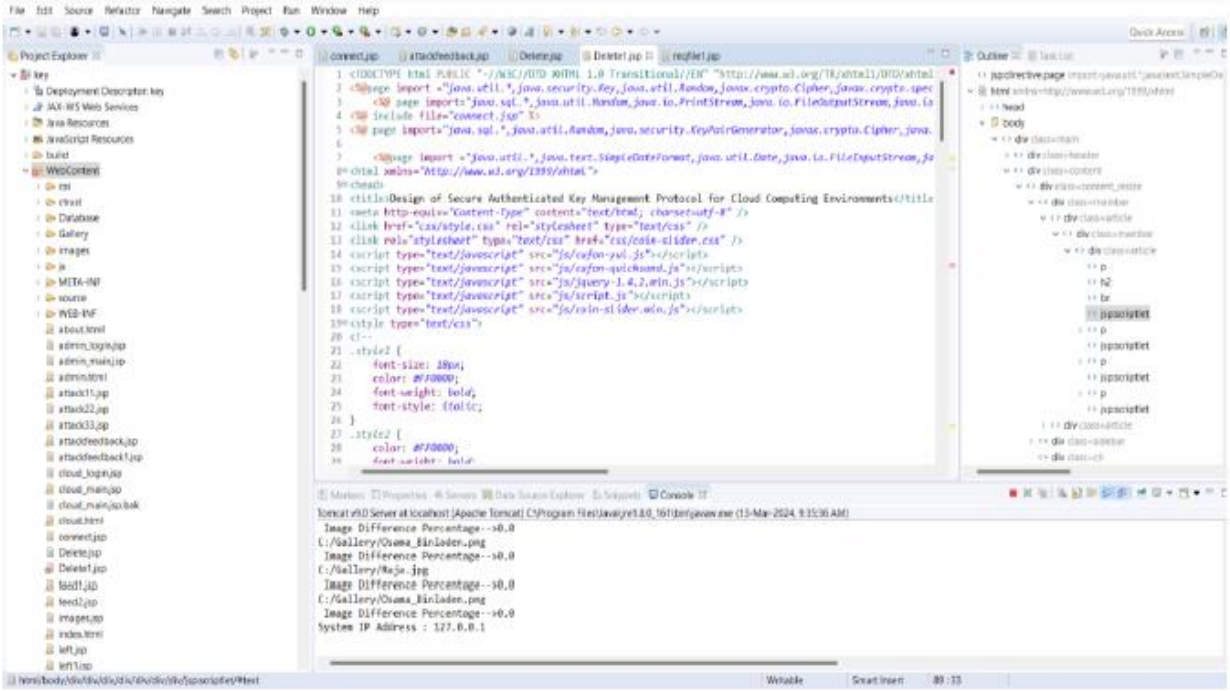

Figure 3

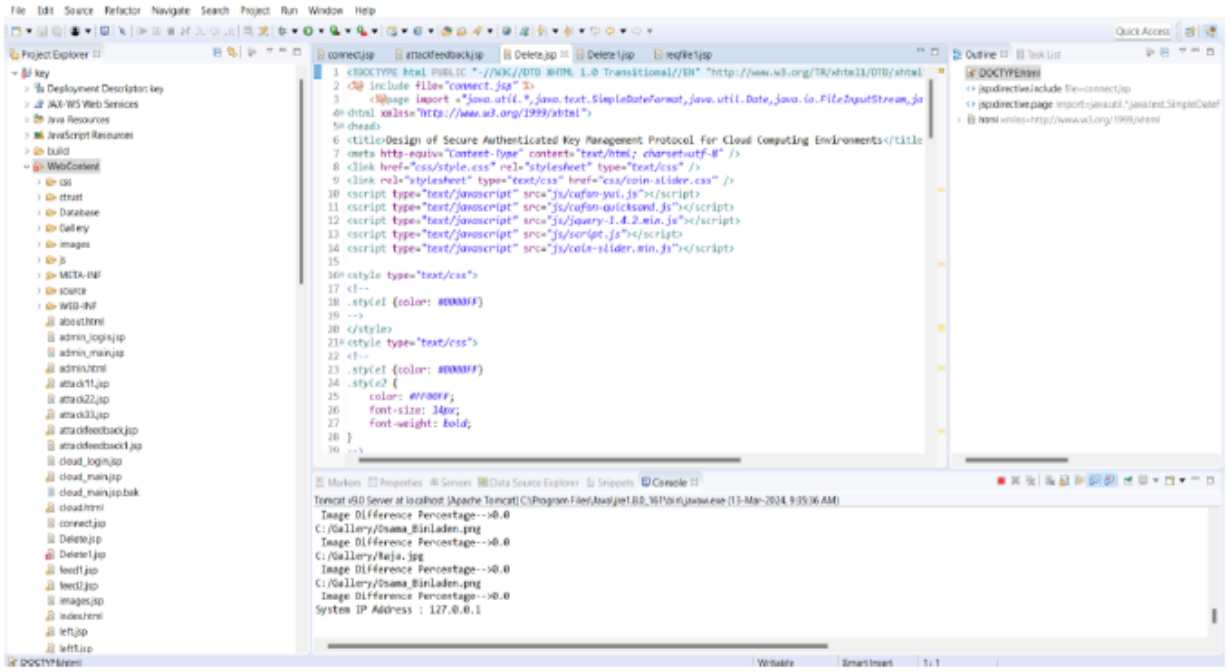

Figure 4

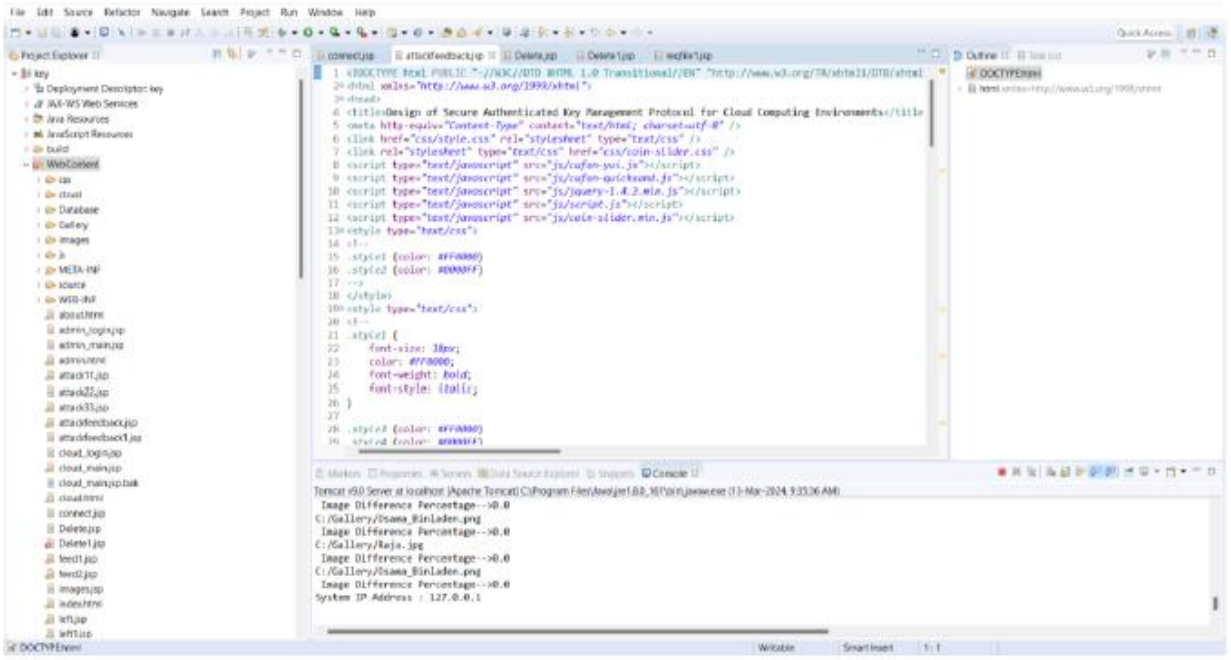

Figure 5

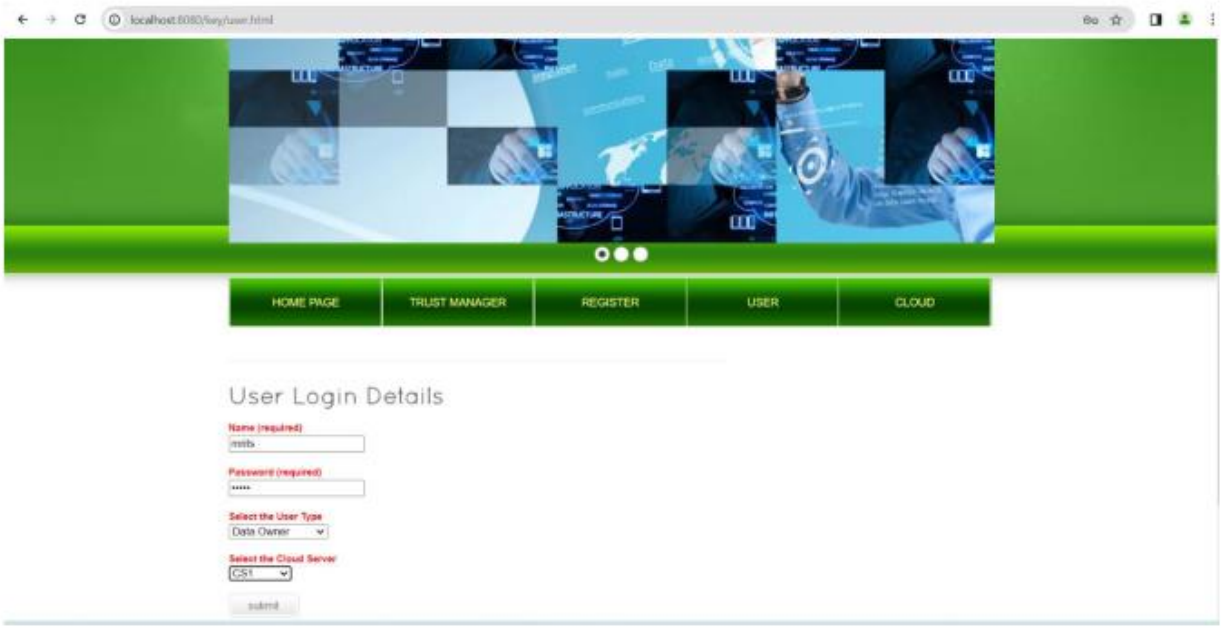

Figure 6

IMPLEMENTATION

DATA OWNER:

In this module, initially the data owner has to get register to the cloud server (CS1,CS2,CS3,CS4) . Data owner will login to the corresponding cloud server he got registered. Data owner encrypt will upload file to the cloud server (CS1, CS2, CS3, CS4) Data owner verifies the file he uploaded either it is safe or not. Data owner can view, how many file has been uploaded to the corresponding cloud servers(CS1,CS2,CS3,CS4) Data owner will send file to trust manager to store the data owner file t5o the corresponding cloud servers (CS1,CS2,CS3,CS4)

CLOUD SERVER:

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud consumer. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

TRUST MANAGER:

Trust manager provides login authorization for both data owner and the end user. Trust manager can view all the cloud status .Trust manager can view the feed backs given by end user and lists all positive and negative feed backs. Trust manager lists no of users in cloud services(IAAS,PAAS,SAAS).Trust manager can view the attackers in cloud servers(CS1,CS2,CS3,CS4) and the no of time attacked.

CLOUD CONSUMER:

Cloud consumer first has to register to the cloud server (CS1, CS2, CS3, CS4) which particular cloud he has to use. Cloud consumer has to login to the cloud he got registered. Cloud consumer feedback about the data (positive or negative feedback)

ATTACKER:

Attacker will view registered users and cloud files
1 **Collusion Attacks** - to mislead feedbacks about the cloud
2 **Sybil Attacks** - When user uses more transaction per day (Exceeds the limit which is assigned by the Trust Manager)

RESULTS

Sample Input:

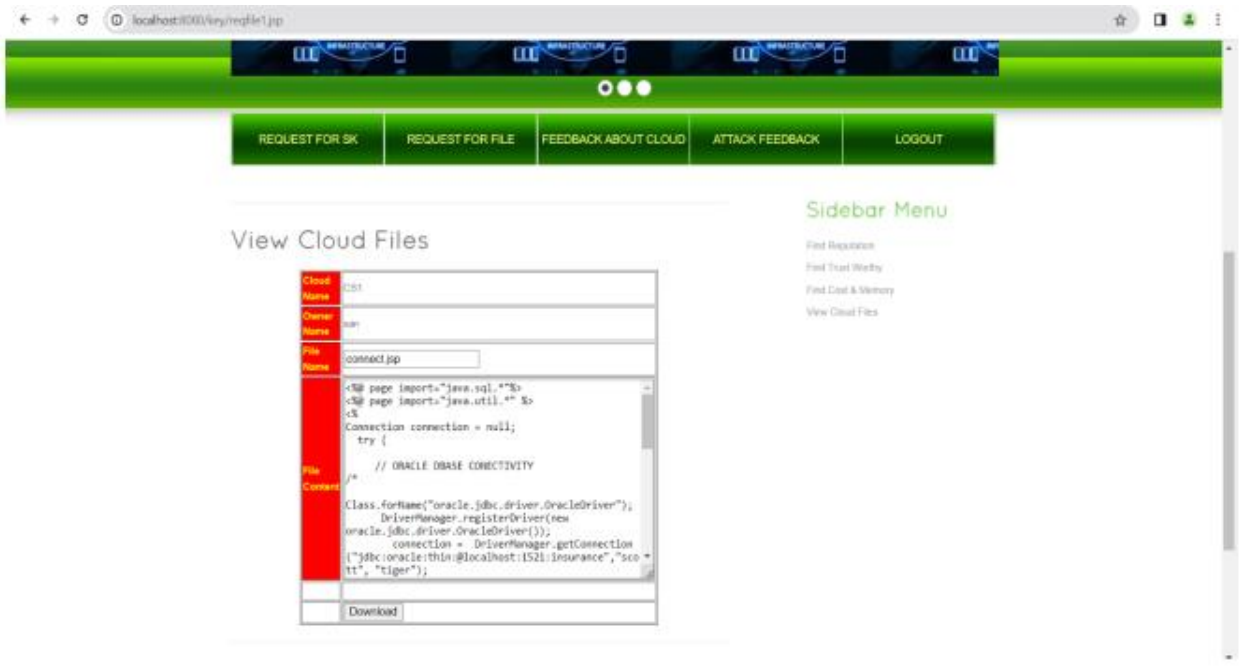

Figure 7

Figure 8

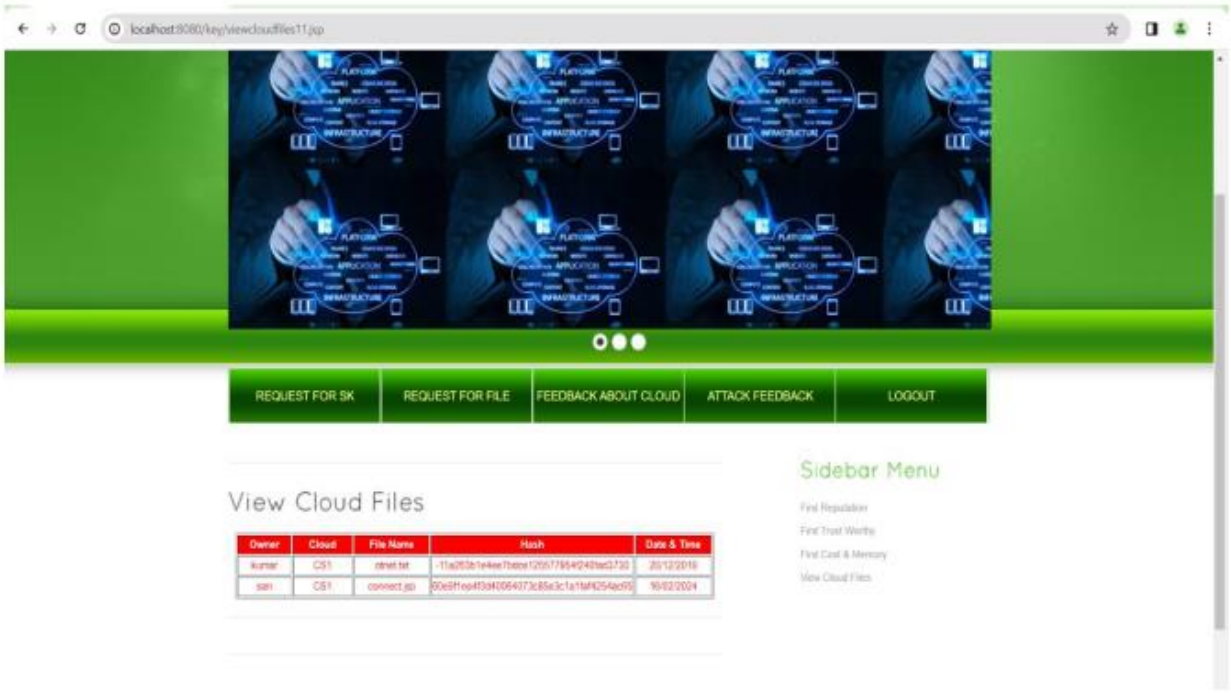

Figure 9

Output:

Figure 10

CONCLUSION

To resist the exhaustion of password attack on the two-factor MAKA protocols, a large number of three-factor MAKA protocols have been proposed. However, almost all threefactor MAKA protocols don't provide formal proofs and dynamic user management mechanism. In order to achieve more flexible user management and higher security, this paper proposes a new three-factor MAKA protocol

that supports dynamic revocation and provides formal proof. The security shows that our protocol achieves the security properties of requirements from multi-server environments. On the other hand, through the comprehensive analysis of performance, our protocol doesn't sacrifice efficiency while improving the function. On the contrary, the proposed protocol has great advantages in terms of the total computation time.

REFERENCES

[1] J. Ronson, So You've Been Publicly Shamed. Picador, 2015.

[2] E. Spertus, "Smokey: Automatic recognition of hostile messages," in AAAI/IAAI, 1997, pp. 1058–1065.

[3] S. Sood, J. Antin, and E. Churchill, "Profanity use in online communities,"in Proceedings of the SIGCHI Conference on Human Factors inComputing Systems. ACM, 2012, pp. 1481–1490.

[4] S. Rojas-Galeano, "On obstructing obscenity obfuscation," ACM Transactions on the Web (TWEB), vol. 11, no. 2, p. 12, 2017.

[5] E. Wulczyn, N. Thain, and L. Dixon, "Ex machina: Personal attacks seen at scale," in Proceedings of the 26th International Conference on World Wide Web. International World Wide Web Conferences Steering Committee, 2017, pp. 1391–1399.

[6] A. Schmidt and M. Wiegand, "A survey on hate speech detection using natural language processing," in Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media. Association for Computational Linguistics, Valencia, Spain, 2017, pp. 1–10.

[7] Hate-Speech, "Oxford dictionaries," retrieved August 30, 2017 from https://en.oxforddictionaries.com/definition/hate speech.

[8] W. Warner and J. Hirschberg, "Detecting hate speech on the world wide web," in Proceedings of the Second Workshop on Language in Social Media. Association for Computational Linguistics, 2012, pp. 19–26.

[9] I. Kwok and Y. Wang, "Locate the hate: Detecting tweets against blacks." In AAAI, 2013.

[10] P. Burnap and M. L. Williams, "Cyber hate speech on twitter: An application of machine classification and statistical modeling for policy and decision making," Policy & Internet, vol. 7, no. 2, pp. 223–242, 2015.

[11] Lee-Rigby, "Lee rigby murder: Map and timeline," retrieved December 07, 2017 from https://http://www.bbc.com/news/uk-25298580.

[12] Z. Waseem and D. Hovy, "Hateful symbols or hateful people? Predictive features for hate speech detection on twitter." in SRW@ HLT-NAACL, 2016, pp. 88–93.

[13] P. Badjatiya, S. Gupta, M. Gupta, and V. Varma, "Deep learning for hate speech detection in tweets," in Proceedings of the 26th International Conference on World Wide Web Companion. International World Wide Web Conferences Steering Committee, 2017, pp. 759–760.

[14] D. Olweus, S. Limber, and S. Mihalic, "Blueprints for violence prevention, book nine: Bullying prevention program," Boulder, CO: Center for the Study and Prevention of Violence, 1999.

[15] P. K. Smith, H. Cowie, R. F. Olafsson, and A. P. Liefooghe, "Definitions of bullying: A comparison of terms used, and age and gender differences, in a fourteen– country international comparison," Child development, vol. 73, no. 4, pp. 1119–1133, 2002.

[16] R. S. Griffin and A. M. Gross, "Childhood bullying: Current empirical findings and future directions for research," Aggression and violent behavior, vol. 9, no. 4, pp. 379–400, 2004.

[17] H. Vandebosch and K. Van Cleemput, "Defining cyberbullying: A qualitative research into the perceptions of youngsters," CyberPsychology & Behavior, vol. 11, no. 4, pp. 499–503, 2008.

[18] H. Vandebosch and K. Van Cleemput, "Cyberbullying among youngsters: Profiles of bullies and victims," New media & society, vol. 11, no. 8, pp. 1349–1371, 2009.

[19] K. Dinakar, B. Jones, C. Havasi, H. Lieberman, and R. Picard, "Common sense reasoning for detection, prevention, and mitigation of cyberbullying," ACM Transactions on Interactive Intelligent Systems (TiiS), vol. 2, no. 3, p. 18, 2012.

[20] P. Singh, T. Lin, E. T. Mueller, G. Lim, T. Perkins, and W. L. Zhu, "Open mind common sense: Knowledge acquisition from the general public," in OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer, 2002, pp. 1223–1237.

[21] H. Hosseinmardi, S. A. Mattson, R. I. Rafiq, R. Han, Q. Lv, and S. Mishra, "Detection of cyberbullying incidents on the instagram social network," arXiv preprint arXiv:1503.03909, 2015.

[22] J. Cheng, C. Danescu-Niculescu-Mizil, and J. Leskovec, "Antisocial behavior in online discussion communities." in ICWSM, 2015, pp. 61–70.

[23] J. Cheng, C. Danescu-Niculescu-Mizil, J. Leskovec, and M. Bernstein, "Anyone can become a

troll," American Scientist, vol. 105, no. 3, p. 152, 2017.
[24] P. Tsantarliotis, E. Pitoura, and P. Tsaparas, "Defining and predicting troll vulnerability in online social media," Social Network Analysis and Mining, vol. 7, no. 1, p. 26, 2017.
[25] S. O. Sood, E. F. Churchill, and J. Antin, "Automatic identification of personal insults on social news sites," Journal of the Association for Information Science and Technology, vol. 63, no. 2, pp. 270–285, 2012.