An Enhanced Authentication Protocol for Cloud Storage-Based Remote Data Access and Sharing in Cyber-Physical-Social Systems Employing CHACHA Method

Ms. Sanjeevini [1], A. Varsha [2], B. Harika [3], S. Vyshnavi [4]

[1] Assistant Professor, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

[2] [3] [4] Student, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

ABSTRACT:

A new paradigm that incorporates the cyber, physical, and social realms is exemplified by cyber-physical-social systems (CPSSs). Providing end-users with proactive, high-quality, and tailored services is the primary objective of CPSSs. Ingenious service reliability frameworks are necessary for CPSSs to do this. Because of its interconnected nature in the physical, digital, and social realms, the cloud computing storage environment need a solid foundation for safe user-cloud communication. The many services offered by cloud storage necessitate efficient, scalable, and secure data management facilities. Cloud service companies impose stringent security measures on their customers that use public cloud storage. Private cloud storage, on the other hand, gives customers the chance to build their own self-managed data security architecture. When it comes to private data sharing and access, this mobile model is in charge. Regardless, it introduces fresh difficulties in terms of data security. Making ensuring that the data storage model is legitimate and safe so that users may access the data in a regulated environment is a censorious concern. There have been several methods created to address this difficulty. However, there is a problem: none of these protocols can provide the necessary level of security efficiency and are open to different types of security assaults. A biometric authentication technique was recently proposed by Tiwari et al. for use in data sharing and access. Their system supposedly withstands serious security breaches. Nevertheless, we demonstrate in this paper that Tiwari et al.'s assertion regarding the

development of a safe method is unfounded, and their protocol is vulnerable to attacks that impersonate both users and servers. Additionally, user anonymity is not provided by the Tiwari et al. approach. For this reason, we provide a method for data access that is more effective, safe, and user-friendly. On top of that, our protocol offers proxy re-encryption, where the cloud server uses the proxy re-encryption key, to allow for data-owner-controlled flexible dissemination. The data owner then creates the credential token to manage the user's access while decryption is happening. According to the results of the security study, our suggested methodology is resistant to a wide variety of security threats. In comparison to other relevant protocols, ours has reasonable communication, storage, and computation costs, according to performance studies. Because of this, our newly developed protocol not only accomplishes the security objectives, but also has performance efficiency that is on par with many other relevant protocols for cloud storage.

INTRODUCTION

In The rapid development of cyber-physical systems (CPSs), which include the Internet of Things (IoT), in recent years has boosted digital innovation and made people's living conditions better. CPSSs, which include the cyber, social, and physical realms, are becoming more pervasive in all parts of our life. One of the main goals of CPSSs is to provide efficient living conditions for people by providing them with high-quality, individualized, and proactive services [1]-[3]. Every moment, the cyber, physical, and social realms contribute to the enormous data deluge that permeates our existence. Data is the central focus of our study; it circulates throughout all three realms and sustains patterns in every facet of our everyday lives. On the other hand, providing CPSSs services isn't very difficult because the massive volumes of data collected from them are often complicated, low-quality, loud, and redundant. [1]. Big data stored in the cloud must undergo thorough scrutiny. Additionally, in order to provide dependable and high-quality services, a cloud computing environment must have secure connectivity. The development of the cloud computing paradigm has given rise to a new form of storage known as cloud storage. There are a number of advantages to using cloud storage, such as public or private cloud data storage, but there are also new concerns about data privacy, protection, and security that come with using the cloud. There is no initial investment required and no chain of risks

towards infrastructure providers with public clouds, which are various practical advantages. People are less interested in using cloud services since they do not have efficient management over networks, data, and security settings. Data privacy, security, and trust are all made more difficult by these factors. Reliability, security, and performance are three aspects of service quality that are mirrored in the private cloud. Also, many businesses may put their own security measures in place with private clouds, rather than relying on the cloud providers'. The utilization of private cloud storage services is mandated whenever delicate data is at stake.

RELATED WORK

‘‘An augmented living environment framework based on tensors for massive services,’’

X. Wang, L. T. Yang, J. Feng, X. Chen, and M. J. Deen, 2016

Significant improvements to human living situations have been brought about by the fast advancements in information, computer, and communication technology. In order to improve people's quality of life, "enhanced living environments" (ELEs) combine cyberspace, physical intelligence, and social interaction. Collaboratively, these areas are called cyber-physical-social systems (CPSSs). Better service frameworks are necessary for CPSSs to offer high-quality services. A sensing plane, a cloud plane, and an application plane make up the architecture described in this piece. The sensing plane cleans and uploads a local tensor representing the object relationships in each local CPSS to the cloud plane. The integration of all local tensors in the cloud plane produces a global tensor. Then, the matching high-quality services are provided by the application plane. The suggested service framework is demonstrated by a case study with a standard CPSS smart house.

‘‘A methodical approach to smart space design that improves user experience,’’

J. Zeng, L. T. Yang, H. Ning, and J. Ma, 2015

The profound impact that smart spaces have on people, computers, and real-world items has led to their rising profile in both academic and business circles. However, real design solutions have failed to prioritize user happiness due to a lack of focus on experience quality in smart space design. We present a methodical approach to smart space design enhancement that incorporates high-level user needs into the design solution. By using an intermediate representation model, we achieve nearly optimal user satisfaction in areas such as locality, energy consumption,

quality of service, and human-computer interaction. Together with the space model and platform library, we also introduce the smart space design platform, which realizes the design flow. In the end, we show that our technique is successful and feasible by using a home health care application.

‘‘Opportunistic software-defined mobile crowdsensing networks,’’

H. Li, K. Ota, M. Dong, and M. Guo,2017

Sharing sensing data acquired by mobile devices like tablets and smartphones is a new paradigm known as mobile crowdsensing. It is challenging to identify a long-term incentive system that recognizes the contribution of every mobile user in network forwarding due to the fact that mobile devices are often linked through an opportunistic network for data transmission. We provide a software-defined opportunistic network architecture for mobile crowdsensing in this study. We plan a command and control system for mobile crowdsensing and opportunistic networks. Through this centralized framework, we are able to solve the optimal decision for sensing service providers and mobile devices, as well as develop an incentive system for data forwarding and collecting in software-defined opportunistic networks. Our incentive system outperforms the original methods, according to the comprehensive simulation findings.

‘‘Challenges and difficulties with cloud security: a literature review,’’

A. Singh and K. Chatterjee, 2017

By utilizing a vast quantity of virtual storage, cloud computing enables the provision of on-demand services via the Internet. Cloud computing's key selling points are its low service costs and the fact that users don't need to invest in costly computer equipment setup. Researchers have been encouraged to explore new related technologies by the increasing integration of cloud computing with many industries and other fields in recent years. Organizations and individuals alike move their data, applications, and services to the cloud because of the scalability and accessibility of its offerings. Despite the benefits, several security risks and challenges have been introduced by the shift from local to remote computing, impacting both consumers and providers. New security risks emerge since many cloud services are supplied by reliable third parties. New security risks emerge as a result of the cloud provider's usage of several web technologies to deliver its services over the Internet. The article covered the fundamentals of cloud computing, including its characteristics,

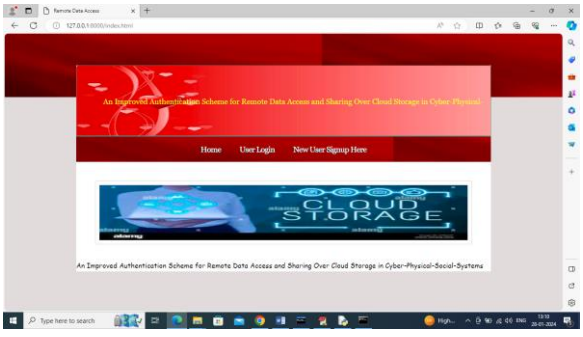
security concerns, risks, and potential remedies. Furthermore, the article delves into other important cloud-related subjects, including the cloud's architecture framework, service and deployment model, technologies, and security ideas, risks, and assaults. Additionally, the study delves into several unanswered questions about cloud security research.

METHODOLOGY

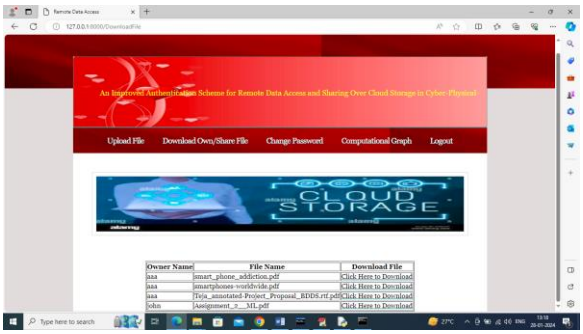
To implement this project, we are using this following Module:

1) User Registration: This module requires users to enter their biometric information, along with a username and password, in order to register with the cloud. The program will then hash the username to protect the user's identity, and it will also hash the biometric image before saving it to the database.
2) User Login/Verification: The data owner or mobile user will be able to access their data page after entering their username, password, and biometric picture in this module. The cloud will then validate all details..
3) Upload File: Users with appropriate login credentials can access encrypted files uploaded by data owners using Elliptic Curve Cryptography (ECC). The cloud server re-encrypts the data before sending it to the share user, who can then decrypt it. In this case, we're using the more than 50% lighter CHACHA extended encryption technique instead of ECC.
4) Change Password: Data owner or mobile user can send request to cloud for password change
5) Download Own/Share File: After the owner or user has verified their identity, they will be able to download the data and decrypt it.
6) Computation Graph: this module, we will compare the proposed ECC and extended CHACHA computation times graphically.

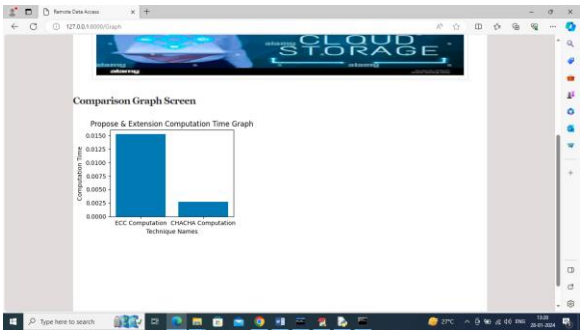
RESULT AND DISCUSSION



In above result click on ‘New User Signup Here’ link to get below signup page



In above result user can view files from all data owners and can click on ‘Click Here’ link to download file and will get below page



CONCLUSION

The protocol developed by Tiwari et al. for use in the cloud storage environment has been cryptanalyzed in this work. Due to the ease with which an attacker might discover the identity of a valid user, their protocol compromises user anonymity. Tiwari et al.'s protocol is susceptible to impersonation attacks on both mobile users and cloud servers. In light of the fact that Tiwari et al.'s protocol is vulnerable to the aforementioned assaults, we suggest a more robust procedure. We officially analyzed the proposed protocol's security using the Random Oracle Model (ROM), and we also provided an informal study to demonstrate the protocol's resilience. Additionally, we compared our protocol's communication, compute, and storage costs to those of comparable protocols, demonstrating that our protocol outperforms the competition.

REFERENCES

[1] X. Wang, L. T. Yang, J. Feng, X. Chen, and M. J. Deen, ‘‘A tensor-based big service framework for enhanced living environments,’’ IEEE Cloud Comput., vol. 3, no. 6, pp. 36–43, Nov. 2016.

[2] J. Zeng, L. T. Yang, H. Ning, and J. Ma, ‘‘A systematic methodology for augmenting quality of experience in smart space design,’’ IEEE Wireless Commun., vol. 22, no. 4, pp. 81–87, Aug. 2015.

[3] H. Li, K. Ota, M. Dong, and M. Guo, ‘‘Mobile crowdsensing in software defined opportunistic networks,’’ IEEE Commun. Mag., vol. 55, no. 6, pp. 140–145, Jun. 2017.

[4] A. Singh and K. Chatterjee, ‘‘Cloud security issues and challenges: A survey,’’ J. Netw. Comput. Appl., vol. 79, pp. 88–115, Feb. 2017.

[5] B. Libert and D. Vergnaud, ‘‘Unidirectional chosen-ciphertext secure proxy re-encryption,’’ IEEE Trans. Inf. Theory, vol. 57, no. 3, pp. 1786–1802, Mar. 2011.

[6] J. Katz and M. Yung, Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings, vol. 4521. Berlin, Germany: Springer, 2007.

[7] J. Hur and D. K. Noh, ‘‘Attribute-based access control with efficient revocation in data outsourcing systems,’’ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[8] W. Li, K. Xue, Y. Xue, and J. Hong, ‘‘TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage,’’ IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 5, pp. 1484–1496, May 2016.

[9] C. Wang, Z.-G. Qin, J. Peng, and J. Wang, ‘‘A novel encryption scheme for data deduplication system,’’ in Proc. Int. Conf. Commun., Circuits Syst. (ICCCAS), Jul. 2010, pp. 265–269.

[10] D. Tiwari, G. K. Chaturvedi, and G. R. Gangadharan, ‘‘ACDAS: Authenticated controlled data access and sharing scheme for cloud storage,’’ Int. J. Commun. Syst., vol. 32, no. 15, p. e4072, Aug. 2019.

[11] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ‘‘Enabling personalized search over encrypted outsourced data with efficiency improvement,’’ IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[12] M. Sookhak, ‘‘Dynamic remote data auditing for securing big data storage in cloud computing,’’ Ph.D. dissertation, Univ. Malaya, Kuala Lumpur, Malaysia, 2015.

[13] D. Thilakanathan, S. Chen, S. Nepal, and R. A. Calvo, ‘‘Secure data sharing in the cloud,’’ in Security, Privacy and Trust in Cloud Systems. Berlin, Germany: Springer, 2014, pp. 45–72.

[14] J. Li, J. Li, Z. Liu, and C. Jia, ‘‘Enabling efficient and secure data sharing in cloud computing,’’ Concurrency Comput., Pract. Exper., vol. 26, no. 5, pp. 1052–1066, 2014.

[15] Y. Chen, L. Song, and G. Yang, ‘‘Attribute-based access control for

multiauthority systems with constant size ciphertext in cloud computing,'' China Commun, vol. 13, no. 2, pp. 146–162, 2016.

[16] Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, ''Secure, efficient and revocable multi-authority access control system in cloud storage,'' Comput. Secur., vol. 59, pp. 45–59, Jun. 2016.

[17] M. Green and G. Ateniese, ''Identity-based proxy re-encryption,'' in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur. Berlin, Germany: Springer, 2007, pp. 288–306.

[18] Q. Liu, G. Wang, and J. Wu, ''Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,'' Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.

[19] J. Zhang and Z. Zhang, ''Secure and efficient data-sharing in clouds,'' Concurrency Comput., Pract. Exper., vol. 27, no. 8, pp. 2125–2143, Oct. 2014.

[20] S. Kamara and K. Lauter, ''Cryptographic cloud storage,'' in Proc. Int. Conf. Financial Cryptogr. Data Secur. Berlin, Germany: Springer, 2010, pp. 136–149