Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 7, No.2, July : 2024

SECURITY & PRIVACY PRESERVING FEDERATED CLOUD COMPUTING CLIENT DESIGN FOR SECURE CHANNEL APPLICATION FOR STORAGE-CLOUD

Dr. Megha Kadam, Associate Professor, Department of Computer Engineering, Marathwada Mitra Mandal's Institute of technology, Lohgaon, Pune
Ms. Mhaske Varsha Dattatraya, Assistant Professor, Computer Engineering, SVPM's College of Engineering, Malegaon(Bk.) , Baramati, Dist- Pune
Dr. Aniruddha S. Rumale, Professor, Information Technology, Sandip Foundations', Sandip Institute of Technology and Research Centre Nashik
Prof. Shital V Bahale, Lecturer, Computer engineering, Government Polytechnic, Murtizapur, Akola
Dr. Dinesh N. Chaudhari, Professor & Dean, Department of Computer Engineering, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal

Abstract
Federated design of client application is considered as the good design for privacy preservation and security by many software scientists. This design principle with intelligent access control can be used to provide security and privacy in application for storage cloud to offer security, privacy, and trust in the utilization of storage cloud. The federated application design uses intelligent access control, advanced encryption, and the secure communication link between cloud service provider(CSP) and users to offer the security and privacy of storage-cloud.
The paper first briefs out the need for federated design using high-level design diagrams to explain the federated structure and behavior of the client application. The Expected results and discussion after the implementation of the design may vary with advancement in base technology used or hardware capacity. The paper discusses the secure client design to establishe the fact that the federated design of an application is reasonably good in offering security and privacy. Using such designs really helps in trusted cloud system.
Keywords: Cloud Computing, Security, Privacy, Trusted Cloud Computing, IAM, Federated design

I. Introduction

Security is one non-ending business as every time one creates some security measure, an intruder come ups with some new method to bypass or break that security measure[1]. Providing security requires many things to consider because many time a security measure itself can become the hurdle in application's usage[2]. Generally, a security breach happens if an intruder gets some information or data necessary for entering the system. Keeping such information in one place and in one piece can make stealing it easy. Federated design promotes the placing data in different chunks at different places. This reduces the risk of entire data theft. And it also guarantees the safety of data and system even some data get stolen by an offender[3].
Cloud computing's three architectures: IaaS[4],PaaS[5], and SaaS[6] require strict implementation of security measures. Security measures[7] plays very important role in ensuring trust[8] among the parties involved in cloud computing: Cloud Service Providers(CSP) and Cloud Users(CU). Federated design places data in scattered and distributed manner, which automatically guarantees, upto some extent, security to data theft[9]. Cloud computing uses SLA(Service Level agreements)s[10], [11] to define the level of trust (security and privacy measures) and type of services with billing procedures. SLA acts as requirement specification and legal binding doc between CSP and CU, but till date, there is no purely SLA based security or design of cloud computing is implemented[12].
The federated design principle uses IAM(Identity and Authentication Manaagement), Machine-fingerprinting, advanced encryption/decryption, and data redundancy to offer maximum security and privacy. Machine-fingerprints are stored on the user's machine itself, causing the possibility of registering as many machines as possible by the user. If we store the data of machine-fingerprints at

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 7, No.2, July : 2024

CSP, the storage and communication overhead involved, limits the number of machines per user. The machine-fingerprint is generated using user's credentials, and machine's unique information[13] to uniquely identify the machine.

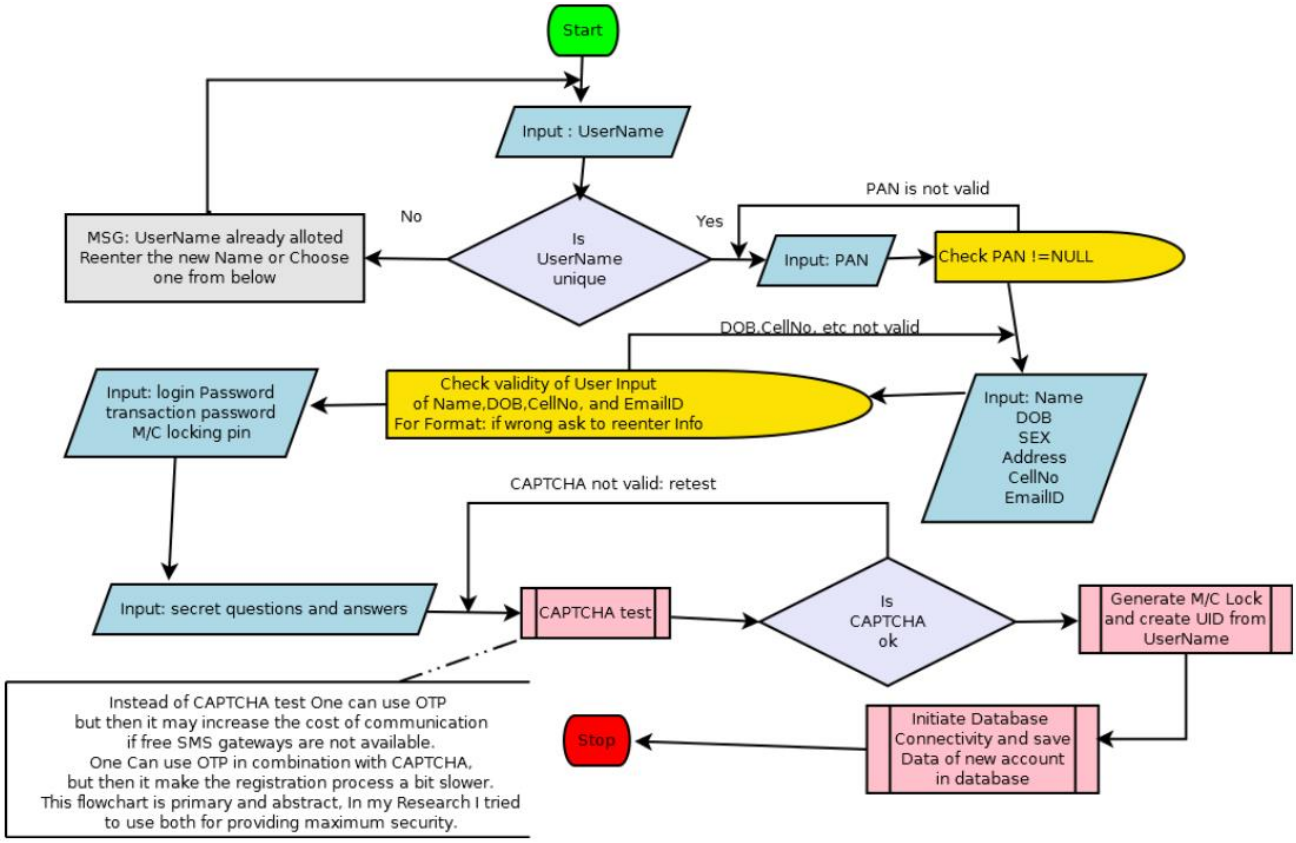

Figure 1: Abstract flowchart for the user registration process of federated client application for storage-cloud

II. Related Conceptual Work of Federated Client Design

The abstract view of the federated client design puts before you the basic flow of system's control and data, refer figure 1. This design assures security at three stages: access control, data at transit, and data at rest[13]. First, a user is authenticated at login process using IAM. Only authenticating the user is not sufficient to sanction him/her the complete unrestricted access to all services. It is also not good for safety of user's account if the account has some confidential or sensitive data. Some parts of user's account and some services need to be kept behind post-login authentication to offer maximum security[14].

If some illegitimate user or third person stole the user's login credentials, then there always remains a chance of abuse of user's account. To avoid this, the concept of user's machine locking using machine-fingerprinting is used, in which the crucial unique identification information of machine is collected by the system at the time of registration and then converted into some unique identification code by combining it with user's credentials. This information is kept in irreversible encrypted format at user's machine itself[15]

Storage of machine-fingerprint at user's machine is preferred as it saves unnecessary maintenance of it at CSP's end and also allows multiple machines to be locked using the machine-fingerprinting[13]. A special algorithm is necessary for the machine-fingerprinting[15]. For new machine-registration/ locking, the process is made quite difficult to be intruded by an illegitimate user as (s)he requires to know many things than mere valid user's username and login password, refer figure 2.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 7, No.2, July : 2024

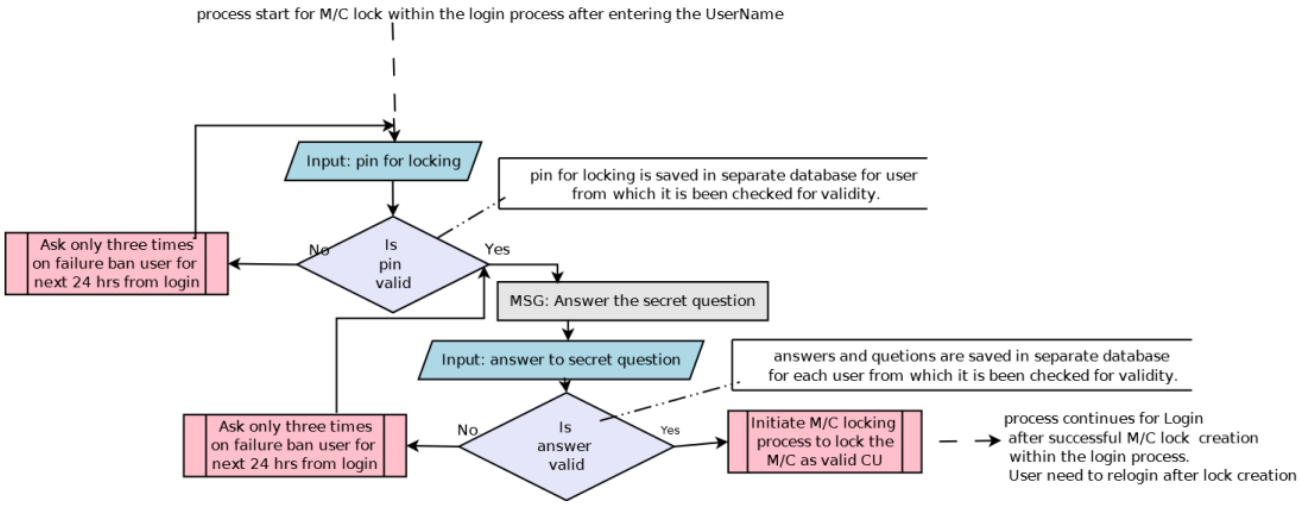

Figure 2: Abstract flowchart for the machine locking process of federated client application within login process

The system generates dynamically the machine-fingerprint at the time of login and compares it with existing (stored lock) machine-fingerprint. Only on correct match user can enter into the system. After which user is offered with secure upload and download of files (data) using advanced encryption schemes like RSA[], SHA[] and data are stored in fragmented and distributed manner at storage-cloud[13], [15]. The complete scenario of 'control and data flow' of federated client design or secure channel is depicted here using high-level abstract designs, refer figure 1, 2, and 3.

Figure 3 shows the login process in its abstract view. While figure2 is the flowchart within the login process, when the machine is yet not locked as Cloud User's client for the user, and user needs to lock it by entering a pin and answering pre-stored answers to secret questions. Secret questions and answers are the part of registration process.

To make registration process secure, a special approach of getting one attribute filled at a time is used. Where next attribute window in registration form gets enabled only after verification and validation of first entry. This slows down the registration process a little bit, but leaves no room for any error in data entry, refer figure1.

Though the storage-cloud itself may not require the database, the CSP need to maintain a database for storing the user information. To store the user information, a federated design of database using mysql or other database need to be implemented, *i.e.* the user information should be stored in different tables and in different location in data-center. Even usernames and passwords should be stored in federated manner in different tables or databases.

Security of data becoming more and more important in this digital age. Today, almost every type of data, from personal to financial, are stored in remote storage-clouds. Banking systems, Googledrive, Microsoft's Onedrive, facebook, whatsapp, etc. . . are the few examples, where one will find data of different types. All of these data need to be kept secure, so that virtually no one except legitimate user, can use it. Access mechanism to these data need to be strong enough, so that no one can login in to the system inadvertently. The federated design of Client is helpful in providing the necessary data security. It also promises the user privacy by making service accessibility only possible through the users' registered device. The machine-locking process can only be countered using hardware cloning, which is non-feasible for the many hackers and intruders.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 7, No.2, July : 2024

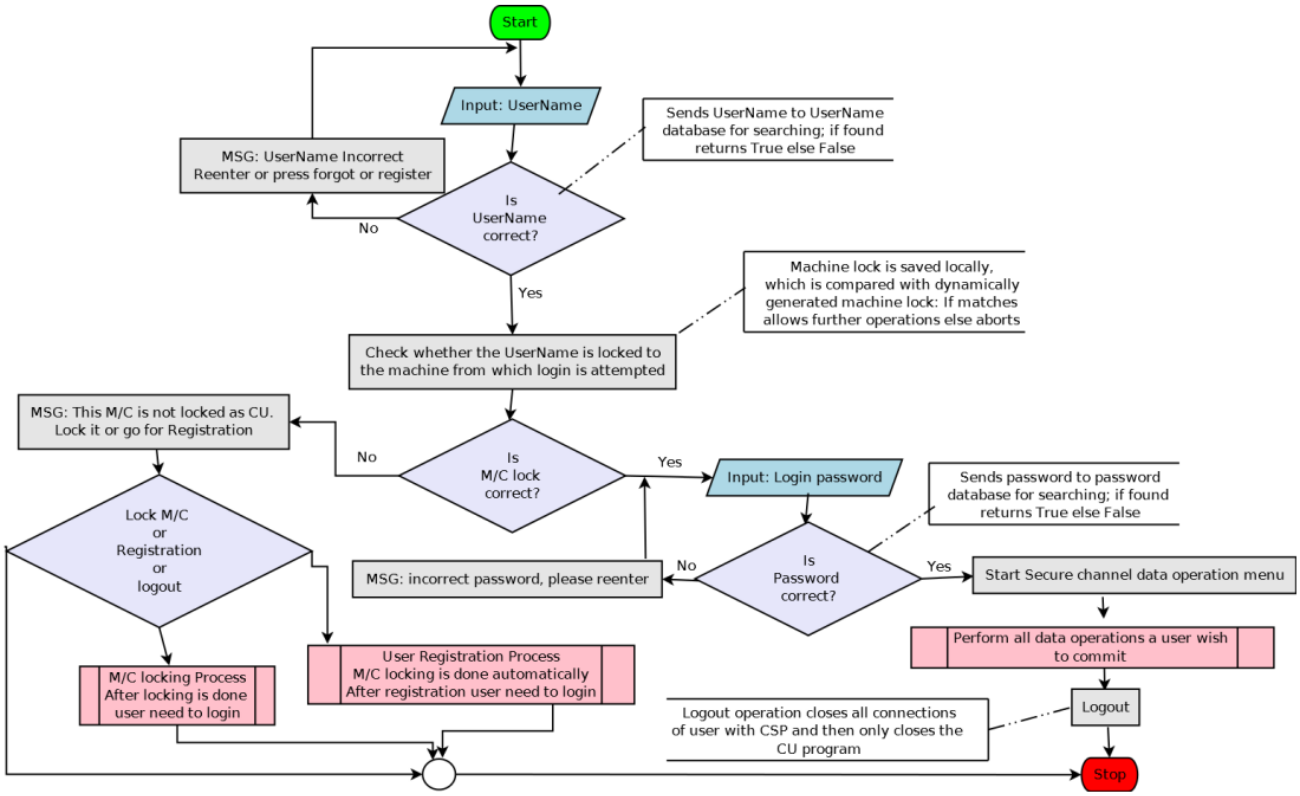

Figure 3: Abstract flowchart for the login process of federated client or secure channel application

III. CONCEPT DISCUSSION

The federated design of secure channel application satisfies this need of security and privacy. The access mechanism is designed in such a way that it is machine locked and require user to enter locking permissions before actual use of any service through client. No service is accessible without the client. This automatically restricts unauthorized access from some unknown machine by some intruder/hacker. The locking code is generated using irreversible encryption algorithm, which considers several factors to create it. Locking code is kept sufficiently long and complex, making it difficult to create it just by intelligent guessing.

The OTP based post authentication or authorization mechanism in federated design of "secure channel application for storage-cloud" restricts the unauthorized user from further entering into the system even if s/he got the primary user credentials. This help in saving confidential and sensitive data of the user from theft or abuse by third party.

For data transfer (upload/download) to/from cloud storage the secure HTTP protocol is used. This provides a security to the transmission. The data is transferred using high end encryption mechanism. This ensures that even if the sniffer or hacker somehow managed to steal the data in transmission, they will hardly get any real data without the decryption keys. At cloud-storage data is stored in federated form over the SAN(Storage Area Network) of storage cloud, making it difficult to access it without the secure channel application. Only through secure channel application, on can reassemble the data scattered in storage-cloud.

Data are stored on storage-cloud using redundancy principle. This obviously help in reassembling it, in case it is not stored correctly or some part of it gone missing. The redundant copy of entire data or part of data can be used to reassemble it for user. Data is stored using user account information to provide compartmentalization to it. This prohibits a user from reading or writing the data from/in other user's account, if data stored is not of public type.

The previous research done by various researchers in providing security to storage cloud missed either one or more point while designing the client program. The federated design of client application successfully combined the required features of security and privacy provision. As Intruders, hackers, and cyber criminals are inventing new ways of attack and data theft every other day, the federated design of secure channel is one of the efficient process of the security and privacy provision. It helps in providing maximum security and trusted computing to the user as well as to the cloud service provider.

The federated design of secure channel is mainly in the Field of IAM to provide maximum security to CUs for Securely storing, retrieving, and sharing their data. There is no such claim made by any researcher in the field of security for perfect and final solution to security. With advancement of technology a cracker or hacker may come up with some intelligent tactics or algorithm to tampered the cloud security. This require the continuous working and research in the field of digital privacy and security.

Failure of present IAM system is possible in future. Continuous work to better the IAM for DCS (Distributed Computing Systems) or 'Cloud computing storage' is needed. This implication emphasizes on finding new and better ways of data encryption/decryption, data sharing, and data storage and retrievals. Future implication is to make the federated design of Secure-channel application for storage cloud as robust as possible.

A better and clear future implications to make secure channel application more better are:

- To Find out more robust algorithms for data encryption and decryption.
- To design a more fine grain architecture of data redundancy than RAID6.
- To develop more intelligent ways for User Identification and authentication.
- Creating a light weight and completely platform independent Secure channel application for storage cloud; and continuously enhancing it.

IV. SUMMARY AND CONCLUSION

The concept of federated design of secure channel application presented is definitely a step ahead in the field of providing better security and privacy to cloud users. The federated design of secure channel application for storage cloud designed here uses intelligent security features of database management, network communication, cryptography, and data redundancy to make the data storage, sharing, and retrieval more safe.

The CSPs need to follow the local as well as Global laws while dealing with client using SLA. Due to the attachment of commerce and law with the cloud computing, the cloud computing is just not a technical venture; rather it is a complete business setup. Proper CSP infrastructure involving operations of cloud requires efficient data center, hardware, secure applications, trained persons, 24 × 7 UPS (Uninterrupted Power Supply) and good building with proper ventilation and cooling systems.

The small companies or individuals, who are using the services of cloud need trust to store their data of any kind on the cloud storage. To built this trust, the cloud access mechanism must be safe. And federated design of secure channel application for storage cloud proposed and presented here, using the existing key technologies, assures the maximum safety to the CUs regarding data storage, sharing, and retrieval. This conclusion is derived because the Secure channel application for storage cloud provides:

- Novel algorithms, novel application and an economical prototype model of IAM;
- Security in data sharing by exploiting the features of secure http for data communication and sharing;
- Security in data storage, retrieval and sharing by applying principles of data redundancy and cryptography;

- User isolation by providing password restricted access to each user with machine locked client applications.

REFERENCES:

[1] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. OReilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472., 2009.
[2] A. Amini, "Secure Storage in Cloud Computing ," immm.sc.-2012-39, Technical University of Denmark , Informatics and Mathematical Modelling , Building 321, DK- 2800 Kongens Lyngby, Denmark, 2012.
[3] Gautam Shroff, *ENTERPRISE CLOUD COMPUTING: Technology, Architecture, Applications*. Cambridge University Press, The Edinburgh Building, Cambridge CB2 8RU, UK, 2010. ISBN 978-0-521-76095-9 Hardback, ISBN 978-0-521-13735-5 Paperback.
[4] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing:
Infrastructure as a service," *International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 23199598*, vol. 1, pp. 1–7, February 2013.
[5] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing:
Platform as a service," *International Journal of Advances in Computing and Communication Technologies (IJACCT)*, vol. 1, no. 1, pp. 46–49, 2014.
[6] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing:
Software as a service," *2nd IEEE International Conference on Electrical , Computer and Communication Technologies, 22-24 February,2017, SVS College of Engineering, Coimbtore, Tamilnadu, India*, pp. 1–6, 02 2017. 978-1- 5090-3239-6/17/$31.00©c 2017IEEE.
[7] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing:
Security issues and measures," *International Journal of Advances in Computer Networks and Its Security IJCNS*, vol. 4, pp. 75–80, 25 June 2014 2014. ISBN: 978-1-63248- 000-2.
[8] Helmut Krcmar and Ralf Reussner and Bernhard Rumpe, ed., *Trusted Cloud Computing*. Springer International Publishing Switzerland, 2014.
[9] S. Berger, R. C. ceres, K. Goldman, D. Pendarakis, R. Perez, J. R. Rao, E. Rom, R. Sailer, W. Schildhauer, D. Srinivasan, S. Tal, and E. Valdez, "Security for the cloud infrastructure: Trusted virtual data center implementation," *IBM J. RES. & DEV.*, vol. 53, no. 4, pp. 1–12, 2009.
[10] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing : Service level agreements(sla)," *INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, ISSN 2229-5518*, vol. 4, pp. 1–5, SEPTEMBER 2013. First presented in Medha 2013 -National Level Conference on Recent Trends in Computer Science, 24th September 2013, Held at JDIET Yavatmal.
[11] R. Buyya, S. K. Garg, and R. N. Calheiros, "SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions," *IEEE International Conference on Cloud and Service Computing*, pp. 1–10, 2011.
[12] P. Wieder, J. M. Butler, W. Theilmann, and R. Yahyapour,
eds., *Service Level Agreements for Cloud Computing*. Springer Science+Business Media, LLC, 2011. ISBN 978- 1-4613-1 -5, e-ISBN 978-1-4614-1 -2.
[13] A. S. Rumale and D. D. N. Chaudhari, "Analysis of secure
channel application for storage-cloud system with existing methods," *Indian Academy of Sciences's SADHANA, published by Springer*, pp. 1–13, 05 2017. Indexed in Wos and Scopus, paper submitted yet not published .
[14] A. S. Rumale and D. D. N. Chaudhari, "IAM with post login authentication of user for service usage authorization in cloud computing," *Inderscience's International Journal of Cloud Computing*, pp. 1–7, 04 2017. Indexed in Scopus and Wos, paper submitted but yet not published .
[15] A. S. Rumale and D. D. N. Chaudhari, "Secure channel
application for storage-cloud system," *IEEE Transactions on Cloud Computing*, pp. 1–8, 05 2017. paper submitted to IEEE TCC but yet not published .