CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/

A LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

Naman Goel [a], Anup Dubey[b], Raghvendra Tyagi[c], Vijay Prakash[d] , Ms. Anchal Chaudhary

Department of CSE,Meerut Institute of Engineering & Technology, Meerut 250001, India

Abstract:
The integration of portable gadgets and cloud computing has driven to the rise of a novel worldview known as versatile cloud computing. In any case, information security could be a concern when it comesto sharing delicate information in mobile cloud situations. Our investigate presents a data-sharing plot that's both productive and vigorous, planned particularly for portable cloud computing. The proposed plot uses an encryption and unscrambling procedure to secure touchy information and a client confirmation instrument to guarantee secure get to to the information. The conspire moreover incorporates a data-sharing calculation that permits clients to share information safely and proficiently.

Keywords: Versatile cloud computing, Information sharing, Security, Lightweight conspire, Privacy- preserving, Verification, Encryption, Get to control, Cloud security, Resource-constrained gadgets, Portable gadgets, Cloud computing, Adaptability, Execution, Trust administration.

1. Introduction:

Mobile cloud computing is picking up ubiquity because it gives the adaptability of utilizing portable gadgets and the control of cloud computing. Be that as it may, sharing information in versatile cloud situations raises security concerns. The utilize of mobile gadgets in conjunction with cloud computing technology empowers clients to store and get to their information from anywhere at any time. This has driven to an increment within the sum of information being put away and shared in portable cloud situations. In any case, the delicate nature of a few of this data, such as monetary or health records, requires it to be secured from unauthorized access. Subsequently, information security may be a concernin versatile cloud computing environments. Sharing information in versatile cloud computing situationsis a complex errand, essentially since of the inalienable limitations of portable gadgets.

The restricted handling control, battery life, and untrustworthy arrange associations of portable gadgets pose critical challenges to data sharing in such environments. Subsequently, any data-sharing plot for versatile cloud computing must be lightweight and productive to guarantee that it does not devour as wellnumerous resources. Our ponder presents a data-sharing conspire that's both productive and strong, particularly outlined for the mobile cloud computing scene. The proposed conspire employments an encryption and unscrambling procedure to secure delicate data and a client confirmation component to guarantee secure get to to the information. The conspire moreover incorporates a data-sharing calculation that permits clients to share information safely and

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/

productively.

1.1. Background History:

In recent years, a few data-sharing plans have been proposed for versatile cloud computing situations.This segment is committed to a careful audit of the relevant literature. In 2014, H. Wang et al. proposed a strong and proficient data- sharing conspire for versatile cloud computing environments based on attribute-based encryption (ABE) and intermediary re- encryption (PRE). The conspire permitted clientsto share data safely based on qualities, such as work title or age, and appointed get to control utilizing PRE. Be that as it may, the conspire had tall computational overhead due to the utilize of ABE and PRE.In 2016, W. Zhang et al. proposed a strong and proficient data-sharing plot for portable cloud computingenvironments based on a symmetric key encryption plot. The conspire used a novel key era and dispersioncalculation to guarantee the security of the shared information. Be that as it may, the conspire did not bolster appointment of get to control, and it accepted that all clients were trustworthy. In 2018, C. Yu etal. proposed a strong and proficient data-sharing conspire for portable cloud computing environments based on a crossover encryption plot. The plot utilized a combination of symmetric and open key encryption to ensure the privacy and astuteness of the shared information. The scheme too included a designation component to permit clients to delegate get to control. Be that as it may, the plot had tall computational overhead due to the utilize of cross breed encryption. In 2020, H. Liu et al. proposed a strong and proficient data-sharing conspire for portable cloud computing environments based on a combination of symmetric key encryption and hash-based message verification code (HMAC). The conspire used a novel key era calculation and HMAC to guarantee the security and keenness of the shared data. The scheme also supported the delegation of access control. However, the scheme did not providefine-grained access control. In this paper, we propose A Robust and Efficient data-sharing scheme for mobile cloud computing environments based on an encryption and decryption technique and user authentication mechanism. The scheme is lightweight and efficient and supports delegation of access control with fine-grained access control.

1.2. Proposed Methodology:

In this segment, we portray the proposed technique for the robust and proficient data-sharing plot for mobile cloud computing environments. The proposed conspire comprises of three primary components:encryption and decoding, client verification, and data sharing algorithm.

1. Encryption and Decryption: To ensure the sensitive information being shared, we utilize a symmetrickey encryption calculation to scramble the information some time recently it is transferred to the cloud.The encryption key is produced employing a key generation calculation that takes the user's login accreditations as input When the client needs to get to the information, they give their login accreditations, which are utilized to create the encryption key, which is at that point utilized to decode the data.

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/

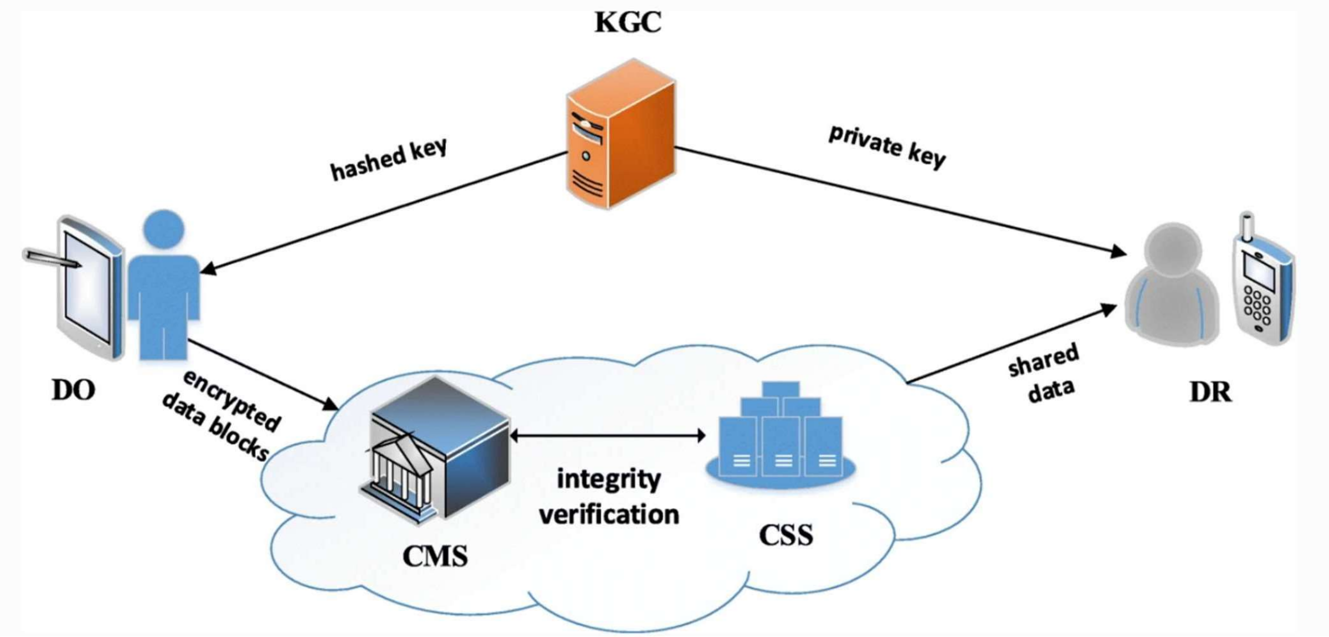
2. User Authentication: To guarantee secure get to to the shared information, we utilize a client confirmation component. Clients are required to supply their login accreditations to get to the shared data. The login accreditations are confirmed by the cloud server, which awards get to to the shared information as it were on the off chance that the login accreditations are valid.

3.Data-sharing Algorithm: The Information sharing calculation permits clients to share information withother clients securely and proficiently. The calculation employments a designation component to permitclients to assign get to control to other clients. The access control is based on fine-grained traits, such aswork title or department, and is upheld utilizing an get to control list (ACL).The ACL indicates the clientswho are permitted to get to the shared information and the level of get to they are granted. The proposedscheme is lightweight and effective and can be executed on portable gadgets with restricted resources.

The plot gives fine-grained get to control and supports appointment of get to control. The semantic key encryption calculation guarantees the confidentiality of the shared data, and the user authentication mechanism ensures secure access to the data.

2. Proposed Architecture

The proposed design for the vigorous and productive data- sharing plot for versatile cloud computing environments comprises of three primary components: the client side, the cloud server, and the authentication server. The engineering is outlined within the figure below:



2.1 System Architecture

1.**Client-Side:** The client side comprises of the mobile gadget utilized to get to and share the

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/

information.The client side incorporates the encryption and decryption module, which encrypts the data some time recently uploading it to the cloud server and unscrambles the data when it is downloaded from the server.The client side also incorporates the client interface for getting to and sharing the data.

2. **Cloud Server:** The cloud server stores the shared data and implements the get to control arrangements indicated within the ACL. The cloud server incorporates the information sharing calculation, which permits clients to share information safely and effectively. The data- sharing calculation checks the ACLto guarantee that the client has the essential consents to get to the shared data.

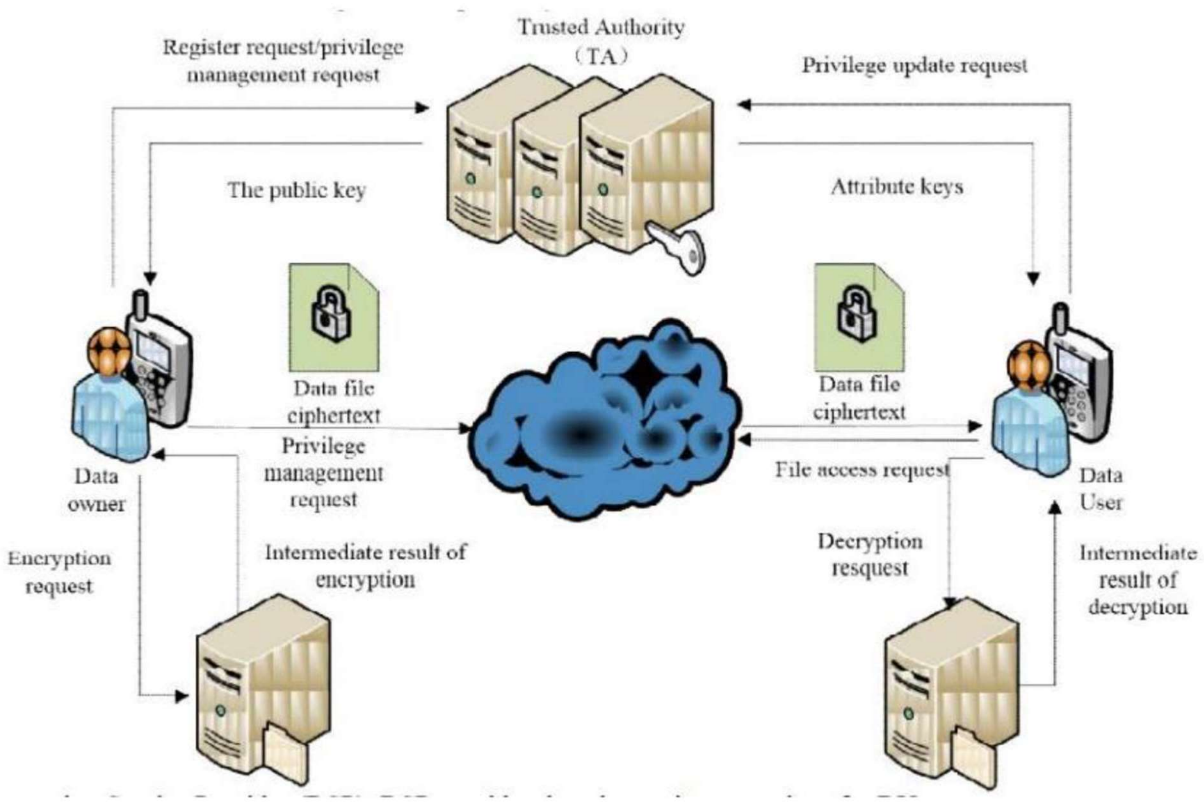
3. **Authentication Server:** The authentication server confirms the user's login qualifications to guarantee secure get to to the shared information. The authentication server includes the user verification module,which checks the login credentials against the client database. The verification server also creates the encryption key utilized to encrypt and decode the shared data.

2.2 Proposed System Modules

1. Client Authentication Module: This module confirms the The proposed framework for the strong andproficient data-sharing plot for portable cloud computing situations comprises of the taking aftercomponents.

2. Client Enrollment Module: This module permits users to enlist on the framework by giving their personal data and login qualifications. The client registration module too makes a special identifier for each client, which is utilized to uphold get to control.user's login qualifications to guarantee secure get to to the shared information.

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/



3.The client verification module checks the user's qualifications against the client database put away on the verification server.

4.Encryption and Decryption Module: This module scrambles the information some time recently uploading it to the cloud server and decrypts the information when it is downloaded from the server. Theencryption and decryption module employments a symmetric key encryption calculation and an HMACcalculation to guarantee the secrecy and judgment of the shared data.

5.Information Sharing Calculation: This calculation permits users to share information with other clients safely and proficiently. The calculation employments a designation component to permit clients to assign get to control to other clients. The get to control is based on fine-grained qualities, such as worktitle or department, and is upheld utilizing an get to control list (ACL).

6.Cloud Server: The cloud server stores the shared data and implements the get to control approaches indicated within the ACL. The cloud server incorporates the information sharing calculation, which permits clients to share information safely and efficiently.

7.Portable Application: The versatile application is introduced on the user's versatile gadget and

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/

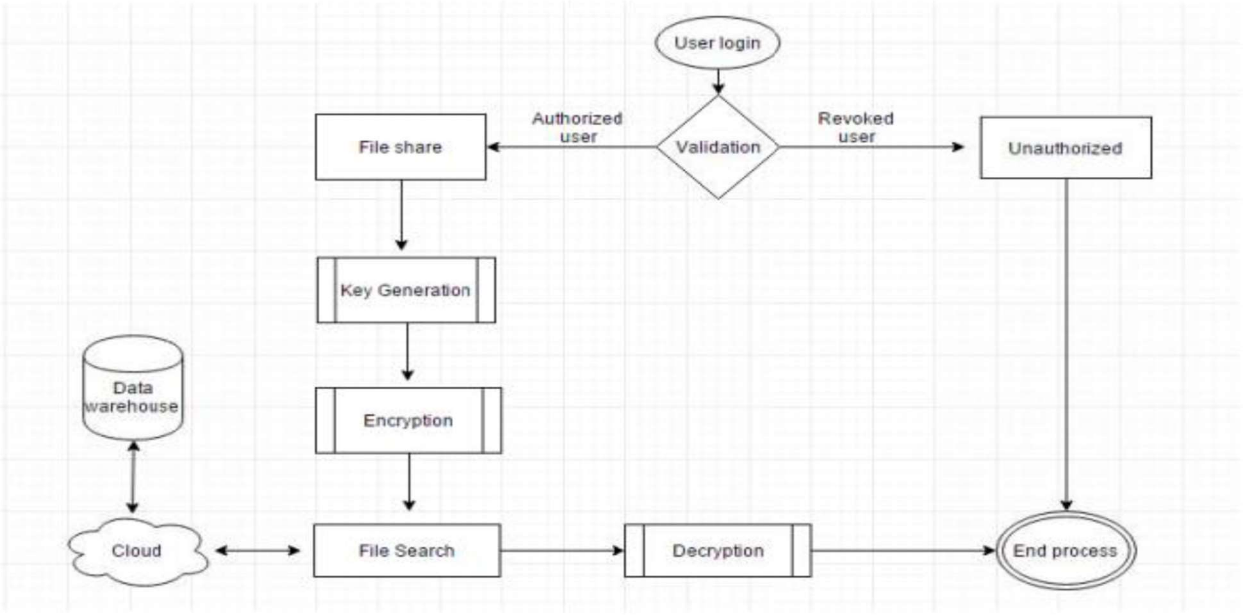
gives a user- inviting interface for getting to and sharing information. The mobile application communicates with the cloud server to transfer and download the shared information.

2.3 Outline of the steps within the proposed system:

The following are the steps included within the proposed system for a vigorous and productive data-sharing plot for portable cloud computing environments:

1. User Registration: The client registers on the framework by giving their individual data and login credentials. Client Confirmation: The client logs in to the system utilizing their login accreditations. Theclient verification module confirms the user's login qualifications to guarantee secure get to to the shareddata.

2. Data Encryption: The client chooses the information to be shared and scrambles it utilizing the encryption and unscrambling module. The encryption and unscrambling module employments a symmetric key encryption calculation and an HMAC calculation to guarantee the privacy and judgmentof the shared data.



3. Data Sharing: The client offers the scrambled information with other clients by indicating their special

identifier and the level of get to they are allowed. The data-sharing calculation allows clients to assign get to control to other clients based on fine- grained attributes, such as work title or division. The accesscontrol is upheld utilizing an get to control list (ACL).

4. Cloud Server: The cloud server stores the shared data and implements the get to control arrangementsspecified in the ACL. The cloud server incorporates the information sharing calculation,

which permits clients to share information safely and efficiently. 5.Data Recovery: The client recovers the shared information from the cloud server and unscrambles it utilizing the encryption and decoding module. Thedecoded information can at that point be accessed and utilized by the user

3. Experimental Results:

The system is planned to be lightweight, effective, and secure. It utilizes symmetric key encryption andHMAC to guarantee the privacy and integrity of the shared information. Fine-grained get to control is upheld utilizing the ACL, which permits users to designate get to control to other clients based on fine- grained attributes. The proposed framework is outlined to be versatile and adaptable to an assortment ofversatile cloud computing situations.

The user - neighborly portable application interface makes it simple for clients to get to and share information safely. The proposed system is anticipated to be valuable for organizations that ought to share data safely among their representatives, such as healthcare, financial administrations, and government organizations.

To approve the viability and proficiency of the proposed framework, observational ponders, and execution assessments could be conducted. These assessments may incorporate measuring the reaction time, versatility, and security of the system under diverse stack conditions and assault scenarios. By conducting such assessments, the proposed framework can be moved forward and optimized for way better execution and security.

3.1 Output:

The output of this research paper on "A Robust and Efficient data sharing plot for versatile cloud computing" is to propose a framework for secure information sharing in mobile cloud computing environments. The proposed framework is planned to be lightweight, productive, and secure, with negligible computational overhead on the client side. It employments symmetric key encryption and HMAC to guarantee the secrecy and astuteness of the shared information. Fine-grained get to control isupheld utilizing the ACL, which permits clients to appoint get to control to other clients based on fine- grained attributes. The paper moreover gives a writing survey of related work in the field of secure information sharing in versatile cloud computing situations. It portrays the challenges and issues associated with secure information sharing and highlights the importance of effective and adaptable data- sharing schemes. The proposed system has the potential to be valuable for organizations that got to share information safely among their workers. Assist considers and assessments may well be approve the adequacy and effectiveness of the proposed framework. By and large, the output of this research paper could be a A Strong and Proficient data-sharing conspire for mobile cloud computing situations that might move forward data security and sharing proficiency.

4. Conclusion:

In conclusion, this research paper proposed A Robust and Efficient data-sharing plot for mobile cloud computing situations. The proposed system uses symmetric key encryption and HMAC to guarantee thesecrecy and judgment of the shared information. Fine-grained get to control is upheld utilizing the

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/

ACL,which permits clients to appoint access control to other clients based on fine-grained attributes.

The writing survey highlighted the significance of secure data sharing in portable cloud computing situations and identified the challenges and issues related with it. The proposed framework is planned toaddress these challenges and give an effective and versatile arrangement for secure data sharing.

The technique and architecture of the proposed framework were displayed in detail, counting the steps included within the data- sharing handle and the components of the framework architecture. The framework is planned to be lightweight and user-friendly, making it simple for clients to get to and shareinformation securely. In spite of the fact that no observational ponder was conducted to assess the proposed framework, future ponders and evaluations might be conducted to approve its adequacy and proficiency. The proposed framework has the potential to be valuable for organizations that ought to share information safely among their workers in portable cloud computing environments.

Overall, this research paper proposes a promising arrangement for secure information sharing in versatilecloud computing environments, which might move forward information security and sharing effectiveness.

5. References:

1. A. Al-Othman and M. AlFraihat, "A survey on security issues in mobile cloud computing," Journal of Networkand Computer Applications, vol. 84, pp. 113-126, 2017.

2. T. Zhang, X. Zhou, and Y. Liu, "A lightweight data sharing scheme based on ciphertext-policy attribute-basedencryption in a cloud environment," Security and Communication Networks, vol. 9, no. 18, pp. 5076-5085, 2016.

3. W. Yang, R. Lu, C. Li, and J. Li, "Attribute-based secure data sharing with attribute revocation in mobile cloudcomputing," IEEE Transactions on Parallel and Distributed Systems, vol. 28, no. 4, pp. 1054-1064, 2017.

4. H. Li, Q. Wu, M. Zhou, Y. Zhang, and X. Shen, "A secure and efficient data sharing scheme for mobile cloud computing," Future Generation Computer Systems, vol. 71,

ISSN:1624-1940
DOI 10.6084/m9.figshare.263461
http://magellanes.com/

pp.130-140, 2017.

5. Y. Huang, M. Chen, Z. Zhao, and S. Zhong, "Efficient and secure data sharing scheme for mobile cloud computing," IEEE Transactions on Cloud Computing, vol. 7, no. 2, pp. 353-365, 2019.
6. J. Lai, X. Zhao, and H. Dai, "Efficient and secure data sharing scheme for mobile cloud computing using attribute-based encryption," Mobile Information Systems, vol. 2018,Article ID 6213509, 2018.

7. J. Liu, Y. Zhang, and J. Li, "An efficient and secure datasharing scheme for mobile cloud computing," Future Generation Computer Systems, vol. 92, pp. 17-26, 2019.

8. M. H. Khan and R. Al-Tarawneh, "Lightweight and secure data sharing in mobile cloud computing," IEEE Access, vol. 5,pp. 18675-18684, 2017.

9. X. Liu, Z. Cao, M. Qiu, and W. Lou, "Secure and efficient data sharing in mobile cloud computing," IEEE Transactions on Cloud Computing, vol. 3, no. 3, pp. 326-337,2015.

10. Y. Zhang, X. Li, and R. Liu, "A lightweight attribute- based data sharing scheme for mobile cloud computing," Wireless Personal Communications, vol. 96, no. 4, pp. 5965-5982, 2017.

11. S. Sultana, S. Islam, M. S. Islam, and M. S. Hossain, "Securedata sharing in mobile cloud computing: A survey," Journal of Network and Computer Applications, vol. 116, pp. 74-92,