iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5639

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

A Lightweight Secure Data Sharing Scheme for Low Power Devices using Mobile Cloud Computing

Prof. Rohini Hanchate[1], Suyash U. Chitnis[2], Avinash S. Mahale[3], Ketan K. Pawar[4]
[1, 2, 3, 4]*Department of Computer Engineering, D.Y. Patil Institute of Engineering and Technology, SPPU, Pune, Maharashtra*

Abstract: ***With the recognition of cloud computing, mobile devices will exchange personal information heterogeneous environment. Consequently, the information security drawback in portable cloud turns into superfluous and extreme which keeps extra improvement of versatile cloud. There square measure substantial studies that are conducted to enhance the cloud security. However, most of them don't seem to be applicable for mobile cloud since mobile devices solely have restricted computing resources and power, to overcome the processing overhead & resources in cloud applications. In this paper, we have a tendency to propose a light-weight information sharing theme (LDSS) for mobile cloud computing. It adopts CP- ABE, associate degree access management technology utilized in traditional cloud atmosphere, however changes the structure of access management tree to create it appropriate for mobile cloud environments. LDSS moves an oversized portion of the process intensive access management tree transformation in CP-ABE from mobile devices to external proxy servers. What is more, to cut back the user revocation value, it introduces attribute description fields to implement lazy-revocation, that could be a thorny issue in program based mostly CP-ABE systems. The experimental results show that LDSS will effectively scale back the overhead on the mobile device aspect once user's square measure sharing information in mobile cloud environments***
Keywords: Mobile cloud computing, Data encryption, Access control, User revocation.

I. INTRODUCTION

With the event of cloud computing and also the quality of good mobile devices, folks area unit step by step obtaining aware of a brand new era of information sharing model within which the information is keep on the cloud and also the mobile devices area unit wont to store/retrieve the information from the cloud. Typically, mobile devices solely have restricted cupboard space and computing power. On the contrary, the cloud has huge quantity of resources. In such a situation, to attain the satisfactory performance, it's essential to use the resources provided by the [01], cloud service supplier (CSP) to store and share the information. Nowadays, varied cloud mobile applications are wide used. In these applications, folks (data owners) will transfer their photos, videos, documents and different files to the cloud and share these information with people (data users) they prefer to share. CSPs conjointly offer information management practicality for information house owners. Since personal information files area unit sensitive, information house owners' area unit allowed to settle on whether or not to create their information files public or will solely be shared with specific information users. Clearly, information privacy of the non-public sensitive information may be a massive concern for several information house owners. The progressive privilege [02], management/access management mechanisms provided by the CSP area unit either not adequate or not terribly convenient. They can't meet all the Requirements of information house owners. First, once folks transfer their information files onto the cloud, they're exploit the information in an exceedingly place wherever is out of their management, and also the CSP could spy on user information for its industrial interests and/or different reasons. Second, folks ought to send [03], Arcanum to every information user if they solely wish to share the encrypted information with bound users that is extremely cumbersome. To alter the privilege management, {the information |the info |the information} owner will divide data users into completely different teams and send Arcanum to the teams that they require to share the information. However this approach needs fine-grained access [04], management. In each cases, Arcanum management may be a massive issue. Apparently, to unravel the on top of issues, personal sensitive information ought to be encrypted before uploaded onto the cloud so the information is secure against the CSP. However, the information coding brings new issues. a way to offer economical access management mechanism on cipher text [05], cryptography so solely the approved users will access the plaintext information is difficult. Additionally, system should supply information house Owners effective user privilege management capability, so that they will grant/revoke information access privileges simply on the information users. There are substantial researches on the difficulty of information access management over cipher-text. In these researches, they need the

subsequent common assumptions. First, the CSP is taken into account honest and curious. Second, all the sensitive information area unit encrypted before uploaded to the Cloud. Third, user authorization on bound information is achieved through encryption/decryption key distribution. In general, we are able to divide these approaches into four categories: straightforward cipher text access management, gradable access management, access management supported absolutely homomorphic coding and access management supported attribute-based encryption (ABE). Of these proposals area unit designed for non-mobile cloud surroundings. They consume great amount of storage and computation resources, that aren't on the market for mobile devices. in keeping with the experimental ends up in [06], the fundamental ABE operations take for much longer time on mobile devices than portable computer or desktop computers. It's a minimum of twenty seven times longer to execute LDSS.

II. LITERATURE SURVEY

1) Paper 1. Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

a) Author Name: Ruixuan Li, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu

b) Description: [13] In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud.

c) Survey: In this paper they uses CP-ABE Encryption Algorithm for securely transmission of data but the main question is why they they go for CP-ABE Encryption Algorithm. There are two types of ABE Encryption Algorithm

i) KP-ABE Encryption Algorithm

ii) CP-ABE Encryption Algorithm KP-ABE :

It is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree Structure the secret key of the user is defined. Ciphertext are labeled with sets of attributes and private keys are associated with monotonic access structures that control which ciphertexta user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications.

d) CP-ABE: Another modified form of ABE called CP-ABE. In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. CP-ABE works in the reverse way of KP-ABE. The access structure of this scheme or algorithm, it inherit the same method which was used in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data; it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is similar to the traditional access control schemes. The encryptor who specifies the threshold access structure for his interested attributes while encrypting a message. It improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt. It can support the access control in the real environment. In addition, the user's private key is in this scheme, a combination of a set of attributes, so an user only use this set of attributes to satisfy the access structure in the encrypted data.

2) Paper 2. Propose Secure and Lightweight Authentication Scheme For IOT Based E-Health Applications

a) Author Name: Maria Almulhim*, Noor Zaman*

b) Description: [14] This research proposed a secure group-based lightweight authentication scheme for IOT based E-health applications, the proposed model will provide mutual authentication and energy efficient, and computation for healthcare IOT based applications. Which will use elliptic curve cryptography (ECC) principles that provide mentioned featured of suggested model.

c) Survey: Increasing use of the IoT services in E-Health application has led to increase the the concern of security and privacy. To overcome with this problem, Data Owner (DO) will add information on cloud gather by the E-Health Devices and the user of these devices will get secure information which is based on CP-ABE Algorithm.

3) Paper 3. A Recent Review on Lightweight Cryptography in IOT

a) Author Name: Effy Raja Naru, Dr. Hemraj Saini, Mukesh Sharma

b) Description: [8] In this review paper, we have focused on different lightweight encryption and decryptions [08], technique used in IoT for secure data transmission. Every technique has some advantage and disadvantage in IoT. Some technique required more storage space but fewer computations and vice versa. Then we compare research status of various lightweight encryption and decryption in IoT. The security problem is a serious issue in IoT and it is hot research topic in IoT.

c) Survey: IoT Application is useful to people but if the IoT system cannot protect the user data from hacker attacks. Lightweight Encryption [07], is a sector of classical cryptography algorithm that is pertinent for resource constraint devices in IoT. Related work for lightweight techniques used for secure data transmission is described in this paper.

4) Paper 4. Implementation of Energy Efficient/Lightweight Algorithm For Wireless Body Area Network

a) Author Name: Azza Zayed Alshamsi, Ezedin Salem Barka

b) Description: [6] Implementation results show that our Lightweight Encryption Algorithm (LEA) is the more suitable for WBAN environment, where the devices used (sensors and mobile devices) have limited memory space and small processing power are very small, than those of conventional encryption algorithms.

c) Survey: This paper aims to provide efficient and effective low Energy communication and lightweight security algorithm design for e-Health monitoring using WBAN. Therefore, our Contribution in two fold. First, conducting an extensive study to determine the best cipher that is suitable for WBAN. Second, determining and [09], implementing the best solution for WBAN in terms of lightweight and energy efficiency which are critical factors in Body Sensor Network. This paper focuses only on the communication between Tier-1 and Tier-2.

5) Paper 5. A Survey On Lightweight Ciphers For IoT Devices

a) Author Name: Merly Annie Philip, Vaithiyanathan

b) Description: [7] In this paper we discuss such existing lightweight block ciphers, PRESENT, KATAN, Humming bird, SIMON, and RECTANGLE and stream ciphers, TRIVIUM, GRAIN, CHACHA, WG-8 and ESPRESSO.

c) Survey: Inherent limitations of size, memory and power limits the devices functionality in secure transmission of sensitive data. The main part of Functionality of these system is the access, storage and transmission [10], of private or personal and sensitive information.

III. PROPOSED SYSTEM

While outsourcing [11], data to cloud, security and efficiency issues should be taken into account. However, it is very challenging to design a secure and efficient mechanism supporting authorization updates. In this paper, we aim to provide a mechanism supporting authorization updates which only incurs a [12], lightweight cost of authorization updates and meanwhile supports a high level of security. This mechanism is consisted of two encryption schemes performed in different layers. The inner-layer encryption scheme is performed on the original plaintext and the generated [04], cipher text is called inner-layer cipher text, while a part of the inner-layer cipher text is encrypted by the outer-layer encryption scheme to generate cipher text, called out-layer cipher text. These two encryption schemes are both performed by data owner. The inner-layer encryption realizes the initial authorization policy, while the outer-layer encryption reflects the updated authorization policy. We implement the proposed mechanism and conduct extensive experiments. The experimental results demonstrate that the proposed mechanism outperforms previous existing approaches, e.g. single-layer encryption and double-layer encryption

We propose LDSS, a [13], framework of lightweight data-sharing scheme in mobile cloud (see Fig. 1). It has the following six components.

1) Data Owner (DO): DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies.

2) Data User (DU): DU retrieves data from the mobile cloud.

3) Trust Authority (TA): TA is responsible for generating and distributing attribute keys.

4) Encryption Service Provider (ESP): ESP provides data encryption operations for DO.

5) Decryption Service Provider (DSP): DSP provides data decryption operations for DU.

6) Cloud Service Provider (CSP): CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

IV. ARCHITECTURE DESIGN

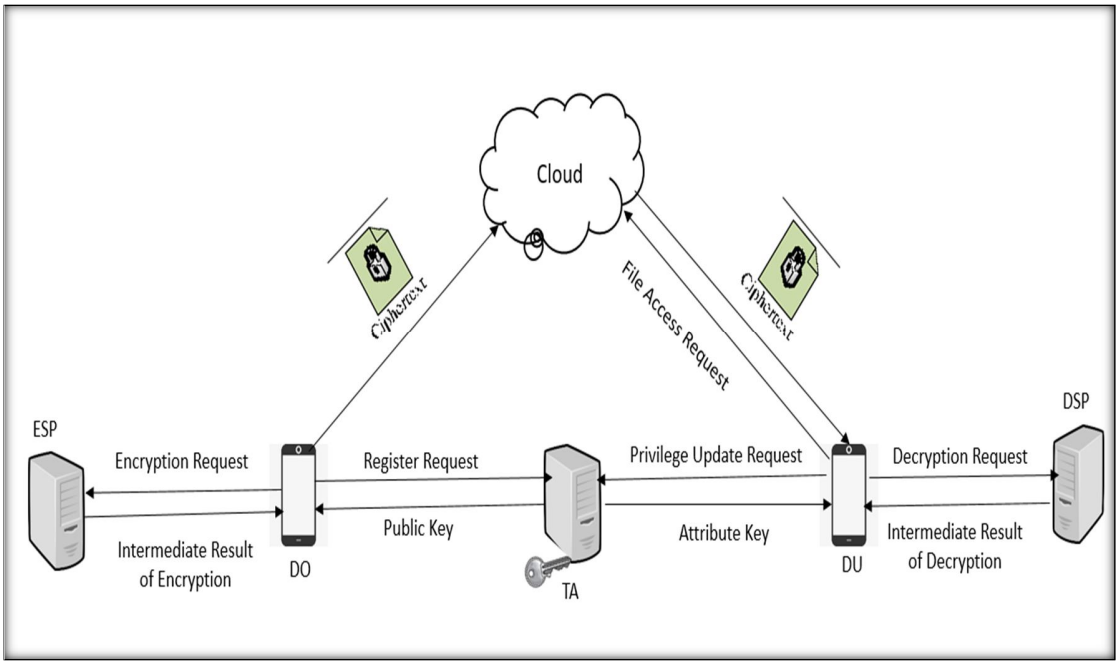


Fig 1. Architectural Diagram for System

A. *System Components*

1) *Data Owner (DO):* DO uploads data to the mobile cloud and share it with friends but direct uploading of data is time consuming so before uploading the data on cloud it needs to be [14], pre-processed on Encryption Service Provider (ESP) and later on giving them attribute upload on cloud.
2) *Data User (DU):* DU retrieves data from the mobile cloud. For receiving data from cloud DU has to send a request to TA and if TA give the Authority to access the data DU able to download the data.
3) *Trust Authority (TA):* TA is responsible for generating and distributing attribute keys. TA is only used to transfer keys (in a small amount) [15], securely between users. TA is online all the time because data users may access data at any time and need TA to update attribute keys.
4) *Encryption Service Provider (ESP):* Everyone is concerned about moving sensitive data to the cloud, and many organizations perceive that the cloud is not as safe as their own data center. If your data is in the cloud, it's not only possible that strangers might see it, but your data could be sitting on the same storage as your competitors. Imagine how much that treasure chest could be Worth? ESP provides data encryption operations for DO. By encrypting the data the data is converted in non-understandable format and with these it is also converted in lightweight data format.
5) *Decryption Service Provider (DSP):* Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. DSP decrypt the data in readable/understandable format and send to DU.
6) *Cloud Service Provider (CSP):* CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud. There are some top most file sharing cloud services like

a) Share File
b) Dropbox Business
c) Google Drive
d) Dropbox
e) Apple icloud
f) SharePoint
g) Egnyte

B. Computation Table

Paper No.	Techniques Used	Working	Transmission Overhead
[1]	LDSS-CP-ABE Algorithm	Securing data with encryption and applying the access control mechanism as well as compression of data	Faster
[2]	RSA Algorithm	Encryption of data without sharing secrete key separately The RSA algorithm can be used for both public key encryption and digital signatures.	Moderate
[3]	C-CP-ABE	It is also work like the LDSS CP-ABE to do attribute based encryption except for lightweight data generation	Moderate
[4]	LEA	It does make the data lightweight , basically used in RFID based systems	Faster

C. Relevant Mathematics Associated With The Project

Consider S is a System. S=I,P,O

Where I= input,

P= Procedure O=Output Input

Data User=Cloud user

Data Owner=Data owner stores data on cloud Trusted

Authority=Authority checks the stored data

Procedure

Process 1 : Data user stores data on cloud.

Process 2 : Data owner processing the data.

Process 3 : Trusted Authority registered the request.

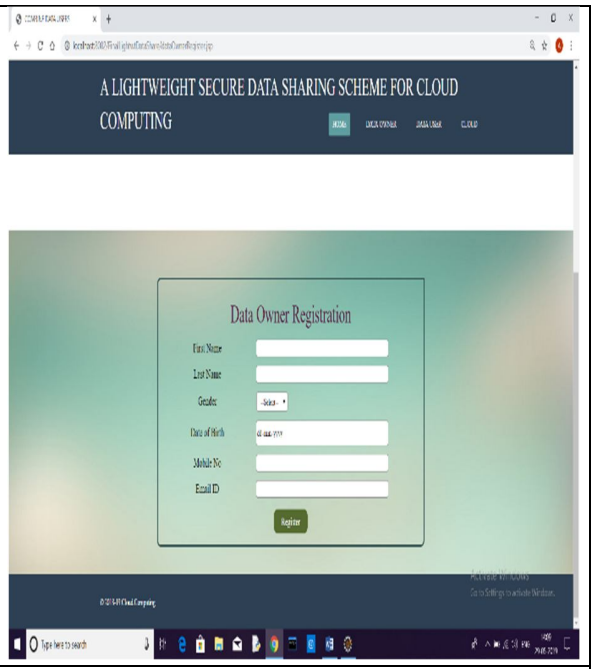
Output:

O= Storing data on cloud securely

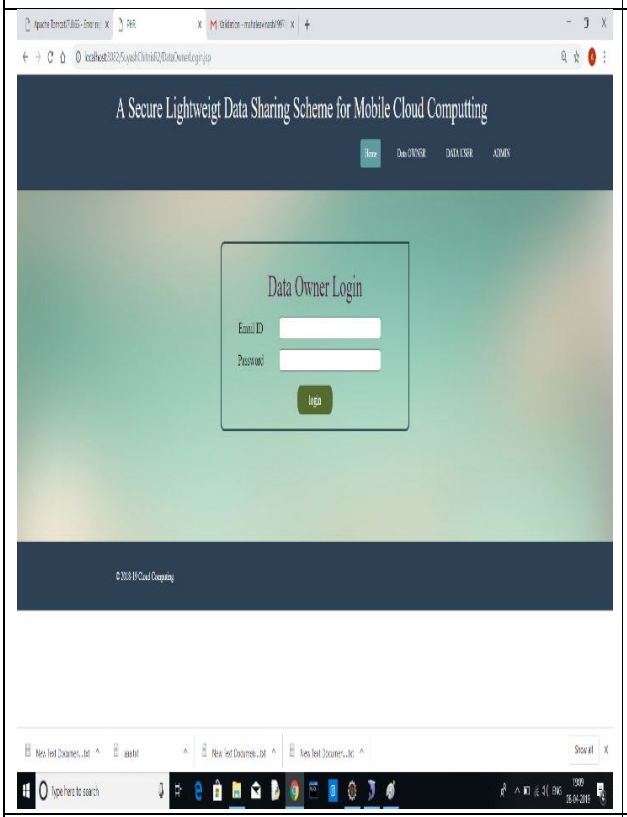
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

D. Implementation Screenshot

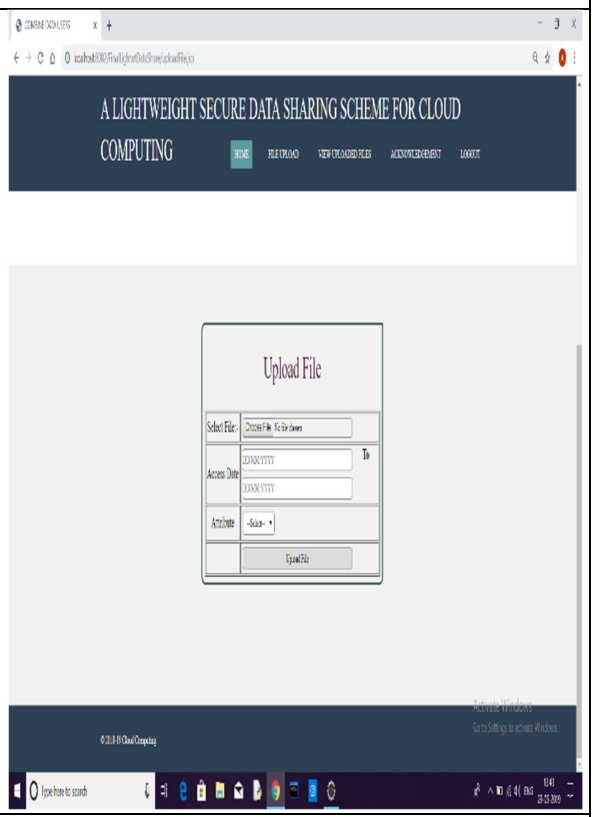
Home Page



Registration Page

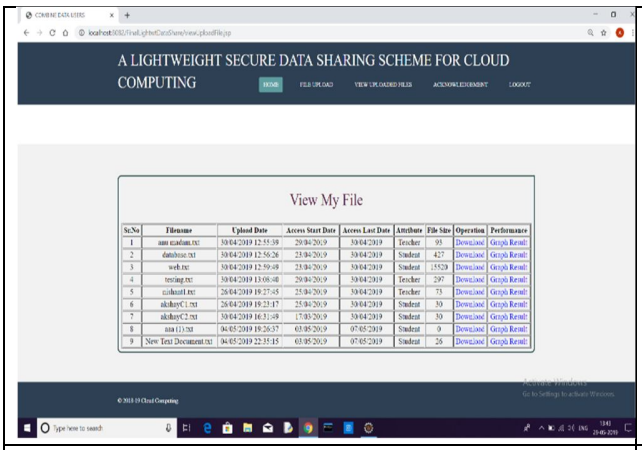


Login Page

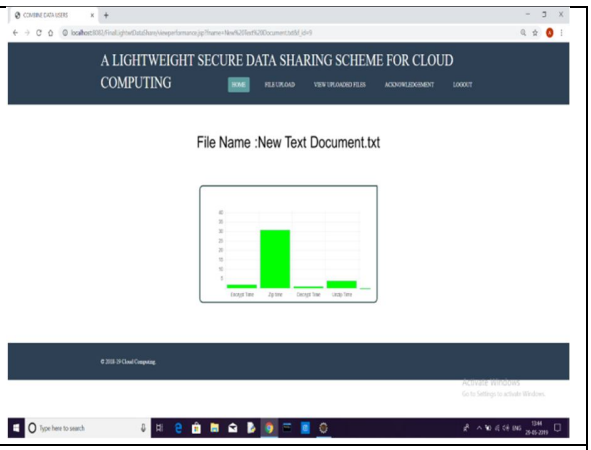


Upload Page

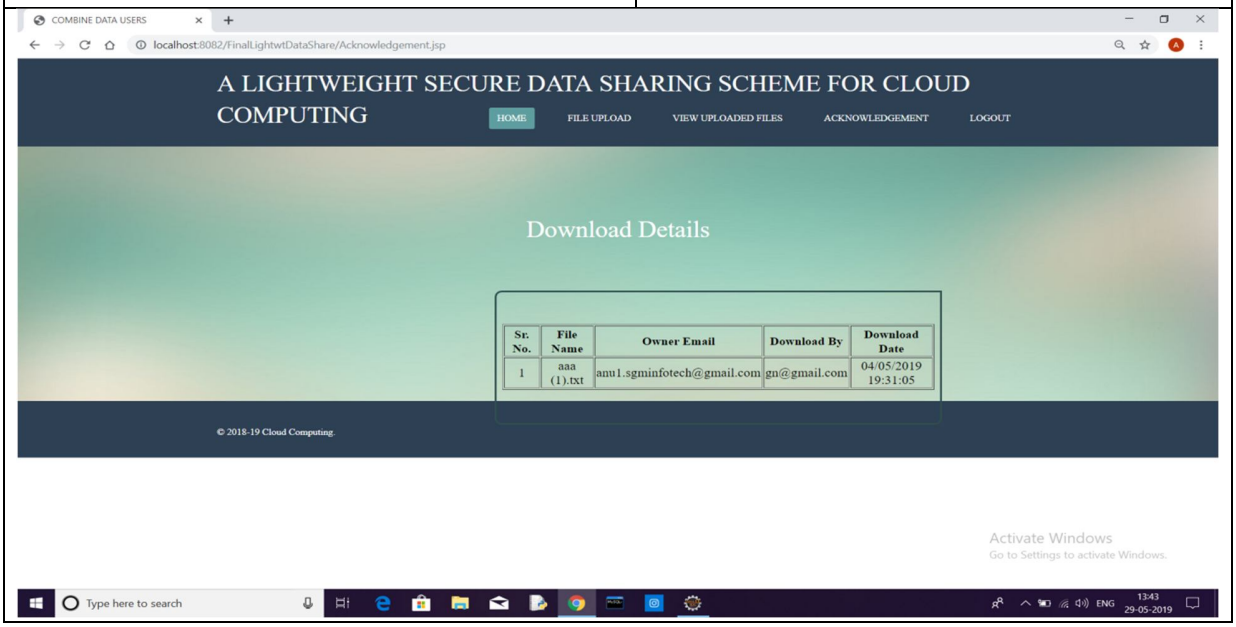
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com



File list



Chart



E. Goals And Objectives

1) The main objective of this study is an important step towards streamlining this effort is to develop a framework and identify necessary properties that a secure and trusted data storing on cloud.

2) Such a framework will allow us to evaluate as well as compare the merits of existing and future data storage on cloud.

3) System should be fully automated.

4) Secure Data Sharing.

V. CONCLUSION

In recent years, several studies on access management in cloud area unit supported attribute-based cryptography rule (ABE). However, ancient ABE isn't appropriate for mobile cloud as a result of its computationally intensive and mobile devices solely have restricted resources. During this paper, we tend to propose LDSS to deal with this issue. It introduces a unique LDSS-CP-ABE rule to migrate major computation overhead from mobile devices onto proxy servers, so it will solve the secure knowledge sharing drawback in mobile cloud

VI. ACKNOWLEDGEMENT

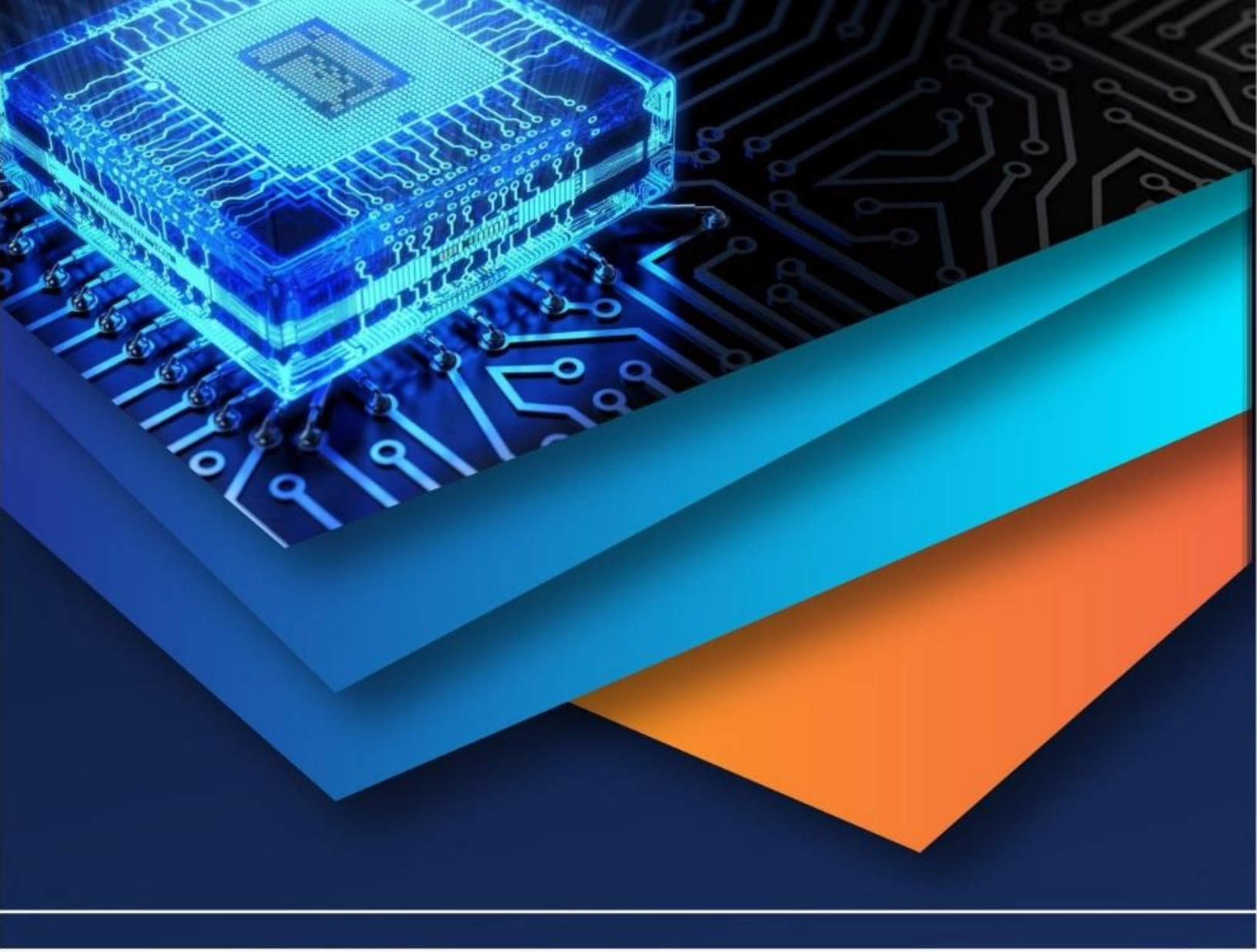
The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We thank to the college authority for providing the required infrastructure and technical support. Finally, we extend our heartfelt gratitude to friends and family members.

REFERENCES

[1] D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing, China: IEEE, pp. 90-98, 2010.
[2] Kan rule, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DAC-MACS: Effective knowledge Access management for Multi authority Cloud Storage Systems. IEEE Transactions on info Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.
[3] Cazorla, Mickaël, Kevin Marquet, and Marine Minier. "Survey and benchmark of lightweight block ciphers for wireless sensor networks." Security and Cryptography (SECRYPT), 2013 International Conference on. IEEE, 2013.
[4] Kan rule, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access management with economical revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.
[5] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. totally secure key-policy attribute-based cryptography with constant-size ciphertexts and quick decipherment. In: Proceedings of the ninth ACM conference on info, laptop and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.
[6] Azza Zayed Alshamsi, Ezedin Salem Barka, Implementation of Energy Efficient/Lightweight Algorithm for Wireless Body Area Network. in 2017 IEEE
[7] Merly Annie Philip, Vaithiyanathan,"A Survey On Lightweight Ciphers For IoT Devices" IEEE International Conference on Technological Advancements in Power and Energy (TAP Energy), pp. 978-1-5386-4021-0/17, 2017
[8] Effy Raja Naru, Dr. Hemraj Saini, Mukesh Sharma,"A Recent Review on Lightweight Cryptography in IOT" in I-SMAC 2017, IEEE.
[9] Manifavas, Charalampos, George Hatzivasilis, Konstantinos Fysarakis, and Konstantinos Rantos. "Lightweight cryptography for embedded systems–A comparative analysis." In Data Privacy Management and Autonomous Spontaneous Security, pp. 333-349. Springer, Berlin, Heidelberg, 2014.
[10] Yu S., Wang C., Ren K., et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA: ACM press pp. 261-270, 2010.

Author Profile

1		**Prof. Rohini Hanchate:** Completed a Master of Engineering degree from Savitribai Phule Pune University and have 6 years of teaching Experience Published 10 International/ National and Conferences papers.
2		**Suyash U. Chitnis :** Pursuing BE in Computer Engineering from D. Y. Patil Institute of Engineering and Technology from Savitribai Phule Pune University.
3		**Avinash S. Mahale :** Pursuing BE in Computer Engineering from D. Y. Patil Institute of Engineering and Technology from Savitribai Phule Pune University.
4		**Ketan k. Pawar :** Pursuing BE in Computer Engineering from D. Y. Patil Institute of Engineering and Technology from Savitribai Phule Pune University.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY