Enhancing Security And Privacy In Cloud Computing Through Attribute-Based Data Sharing

Syed Safiya Tahaseen[1], D.murali[2]

#1Student,Department of CSE, CSE dept. QUBA college of engineering & Technology, Venkatachalam, Nellore,AP, India

#2 Assistant Professor, Department of CSE, QUBA college of engineering & Technology, Venkatachalam, Nellore,AP, India

Abstract_ Data sharing is a handy and financial provider provided via cloud computing. Data contents privateness additionally emerges from it when you consider that the facts is outsourced to some cloud servers. To shield the precious and touchy information, more than a few methods are used to decorate get admission to manipulate on the shared data. In these techniques, Ciphertext-policy attribute-based encryption (CP-ABE) can make it extra handy and secure. Traditional CP-ABE focuses on information confidentiality merely, whilst the user's non-public privateness safety is an vital trouble at present. CP-ABE with hidden get entry to coverage ensures records confidentiality and ensures that user's privateness is no longer published as well. However, most of the present schemes are inefficient in verbal exchange overhead and computation cost. Moreover, most of these works take no consideration about authority verification or the hassle of privateness leakage in authority verification phase. To handle the troubles stated above, a privateness maintaining CP-ABE scheme with environment friendly authority verification is delivered in this paper. Additionally, the secret keys of it acquire consistent size. Meanwhile, the proposed scheme achieves the selective safety underneath the decisional n-BDHE trouble and decisional linear assumption. The computational effects affirm the deserves of the introduced scheme.

Index Terms—Attribute-based encryption (ABE), authority verification, hidden access policy, privacy preserving.

1.INTRODUCTION

Cloud methods make it viable to make use of statistics science sources into commercial enterprise domain. The cloud presents range of scalable offerings on-demand, such as on-line databases, software interface, storage and computing resources, etc. Users can reap offerings thru phones, laptops, and computers . Cloud storage presents far off facts storage and administration

services. It is additionally useful in records examining and computing, which is pretty easy as it can grant a variety of offerings at the equal time. Cloud has many blessings in information storage, such as lowering conversation fee and preservation charge, saving resources, permitting far flung access, and so on. However, humans may now not be inclined to keep their information in the cloud, even even though it offers so many advantages due to the fact of the records confidentiality and privateness problems. The cloud server (cs) may also be untrusted, in different words, if records is uploaded to cloud, the cloud provider issuer might also acquire and expose users' non-public privacy, and even get entry to and share the records illegally [1]. To make certain the confidentiality of the facts in cloud, human beings are inclined to encrypt them earlier than they are uploaded to cloud. But the prevalent encryption algorithms make the statistics technique emerge as difficult. Abe is a precise candidate to overcome this limitation. Abe was once first proposed in 2005 with the aid of sahai and waters [2], which assured the information confidentiality and furnished the fine-grained get right of entry to manage coverage to the customers. It has been extensively regularly occurring as an wonderful approach encrypting the outsourced records in cloud computing. Abe improves the effectivity when the records owner (do) intends to share facts contents with multiusers. It lets in do to specify an get admission to coverage to the encrypted files, which can make the customers who healthy it, get admission to uploaded data.

The customers who do now not fulfill the get admission to shape can't get any records about the statistics contents. For instance, we reflect onconsideration on the records get right of entry to manipulate for a company. If the ceo intends to publish a labeled file, via the cloud, to the managers in income department, planning department, and lookup and improvement (r&d) department. Then he/she can use an abe scheme. First he/she encrypts the file and specifies an get right of entry to shape as ω = supervisor ∧ (sales branch ∨ planning branch ∨ r&d). Next he/she uploads the encrypted file and the get right of entry to shape into the cs. Only the managers in the three referred to departments can get admission to the categorized file, and the managers in different departments or the conventional body of workers in the three stated departments can't analyze some thing about the file even if they collude. Most of abe proposals function very properly

in impervious statistics sharing. However, the private privateness of the do and the customers is not noted in these constructions. For comfort of getting better data, the get admission to coverage is usually despatched with ciphertexts. In some scenarios, the get right of entry to shape may also raise touchy records of users. For instance, a affected person wishes to share his/her non-public fitness report (phr) with some docs and household members, however he/she might also now not choose others to understand that he/she is sick. If the affected person employs a regular abe scheme to encrypt the phr, even though the malicious person can't get the contents of the phr, he/she may additionally get some data about the customers as proven in fig. 1. The get entry to coverage includes “cardiopathy” and “dc hospital” and the malicious 1/3 celebration may additionally bet that the do is struggling from a coronary heart assault and is treating in the dc hospital. Hence a herbal hassle is how to hold the shared facts secure, whilst the privateness of them is additionally protected.

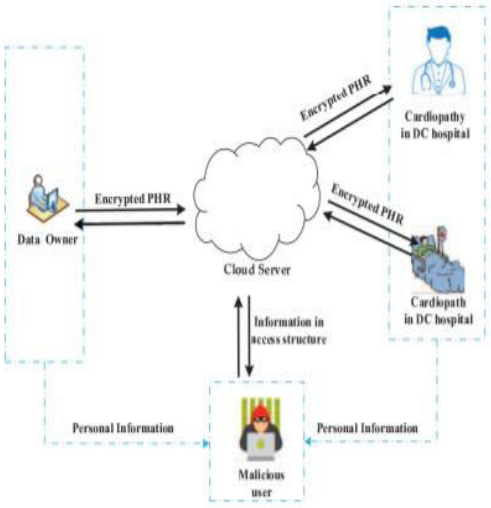

Fig 1:Privacy Leakage Model

2.LITERATURE SURVEY

2.1) Mobile cloud computing: A survey

AUTHORS: N. Fernando, S. W. Loke, and W. Rahayu

Despite increasing usage of mobile computing, exploiting its full potential is difficult due to its inherent problems such as resource scarcity, frequent disconnections, and mobility. Mobile cloud computing can address these problems by executing mobile applications on resource providers external to the mobile device. In this paper, we provide an extensive survey of mobile cloud computing research, while highlighting the specific concerns in mobile cloud computing. We present a taxonomy based on the key issues in this area, and discuss the different approaches

taken to tackle these issues. We conclude the paper with a critical analysis of challenges that have not yet been fully met, and highlight directions for future work.

2.2) Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges

AUTHORS: S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya

Recently, Cloud-based Mobile Augmentation (CMA) approaches have gained remarkable ground from academia and industry. CMA is the state-of-the-art mobile augmentation model that employs resource-rich clouds to increase, enhance, and optimize computing capabilities of mobile devices aiming at execution of resource-intensive mobile applications. Augmented mobile devices envision to perform extensive computations and to store big data beyond their intrinsic capabilities with least footprint and vulnerability. Researchers utilize varied cloud-based computing resources (e.g., distant clouds and nearby mobile nodes) to meet various computing requirements of mobile users. However, employing cloud-based computing resources is not a straightforward panacea. Comprehending critical factors (e.g., current state of mobile client and remote resources) that impact on augmentation process and optimum selection of cloud-based resource types are some challenges that hinder CMA adaptability. This paper comprehensively surveys the mobile augmentation domain and presents taxonomy of CMA approaches. The objectives of this study is to highlight the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. We present augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based. We critically analyze the state-of-the-art CMA approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present a taxonomy. Vital decision making and performance limitation factors that influence on the adoption of CMA approaches are introduced and an exemplary decision making flowchart for future CMA approaches are presented. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions.

2.3) Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems

AUTHORS: R. Kumar and S. Rajalakshmi

The concepts of Cloud computing are naturally meshed with mobile devices to enable on-the-go functionalities and benefits. The mobile cloud computing is emerging as one of the most important branches of cloud computing and it is expected to expand the mobile ecosystems. As more mobile devices enter the market and evolve, certainly security issues will grow as well. Also, enormous growth in the variety of devices connected to the Internet will further drive security needs. Understanding the true potential of mobile cloud computing and identifying issues with mobile cloud security, privacy, feasibility and accessibility remain a major concern for both the customers and the enterprises. This paper covers the mobile cloud security issues and challenges by looking at the current state of cloud security breaches, vulnerabilities of mobile cloud devices, and how to address those vulnerabilities in future work in aspect of mobile device management and mobile data protection. Also, it highlights on usage of SCWS (Smart Card Web Services) rivalry to intensify security of mobile cloud computing.

3.PROPOSED SYSTEM

- Motivated by the above-mentioned challenges and based on [24]–[26], we introduce an CP-ABE scheme with efficient authority verification, which is used to help the user determine whether he/she is authorized or not. The test technique comes from the Abdalla's verifiable random functions with the auxiliary information [14], where the auxiliary information is used to generate the test parameters. The proposed scheme can solve the ciphertexts verification without disclosing the privacy of the users.
- A framework of CP-ABE scheme with efficient authority verification is proposed, which guarantees the data confidentiality and protects the user personal privacy as well.
- In order to avoid unnecessary computations of users in decryption algorithm, we design an authority identification method, which can help the user verify whether he/she is an

authorized one and decrypts successfully.

- The proposed scheme achieves constant private key size, which is independent of user's attribute number. It reduces the cost of transmission and storage.
- In addition, a compact security analysis by using a sequence of hybrid games is given to show the proposed scheme of how to achieve anonymity, which is lacking in most of the existing works.

3.1 IMPLEMENTATION

DATA OWNER

In this module, data owner has to register to Authentication Center and Authentication Center checks and authorizes the data owner login . Data owner browse the file , encrypt and upload file with its mac. Once uploaded the file all the authentication center must provide the storage access for the file store on the cloud. Data owner can also delete the file after the uploading of the file to the cloud.

Authentication Center

In this module Authentication Center checks user & owner login and authorizes the registration. Authentication center list all other sub-authentication centers and provide authorization (Activate OR Deactivate). Authentication center provides the storage access to cloud for every file uploaded by the data owner.

AA 1

In this module the AA1 shows all the private key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

AA 2

In this module the AA2 shows all the public key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

Cloud Server

Receive all files from the data owner and store all files, user details. Provide files to end user after verifying Private key and secret key provided by the authentication center. Maintain file transaction details and forward the file download request from the user to the authentication centre.

End User (Receiver)

In this module end user has to register and login, and the user is authorized by the authentication center, user will request private key from the AA1 and the secret key from the AA2 to download the file from cloud server.

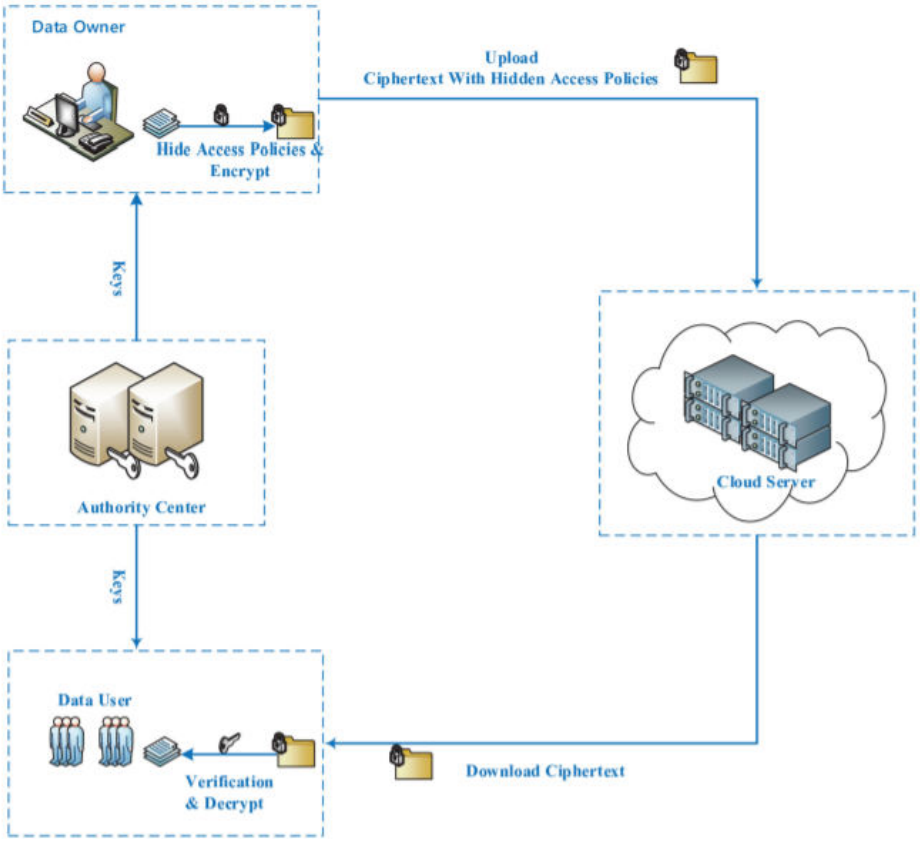

Fig 2:System Model

4.RESULTS AND DISCUSION

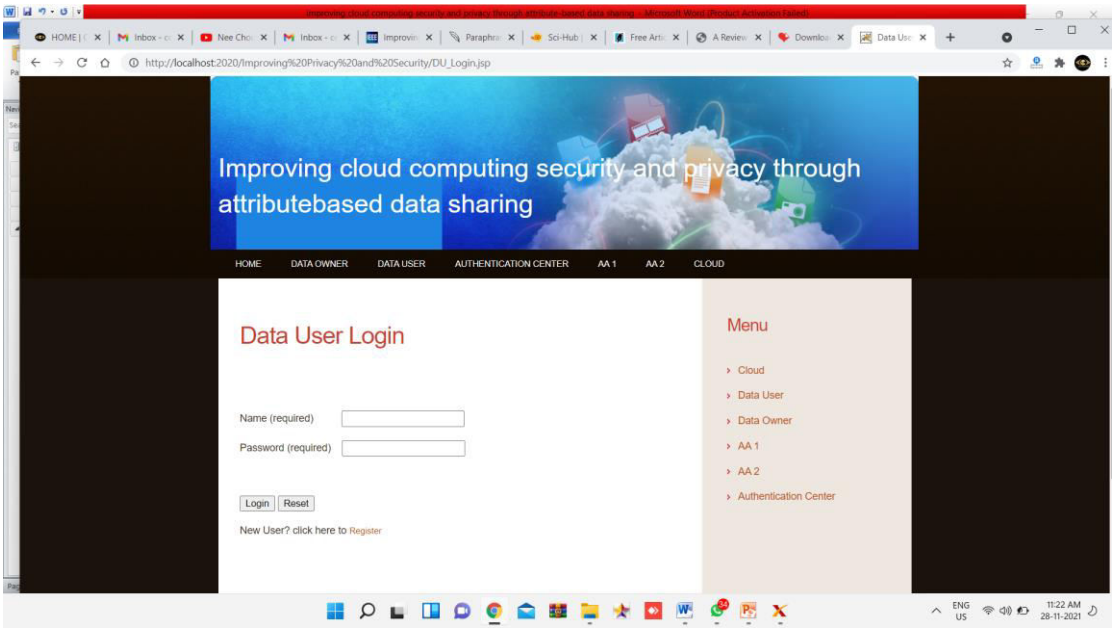

Fig 4.1 Data user Login form

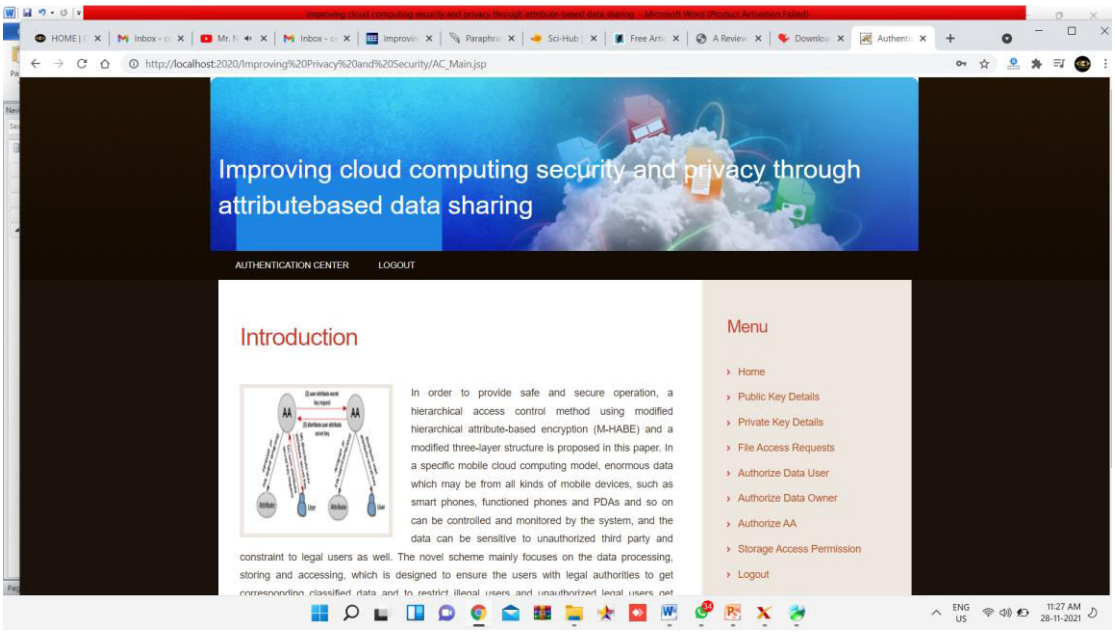

Fig 4.2 Authority Home Page

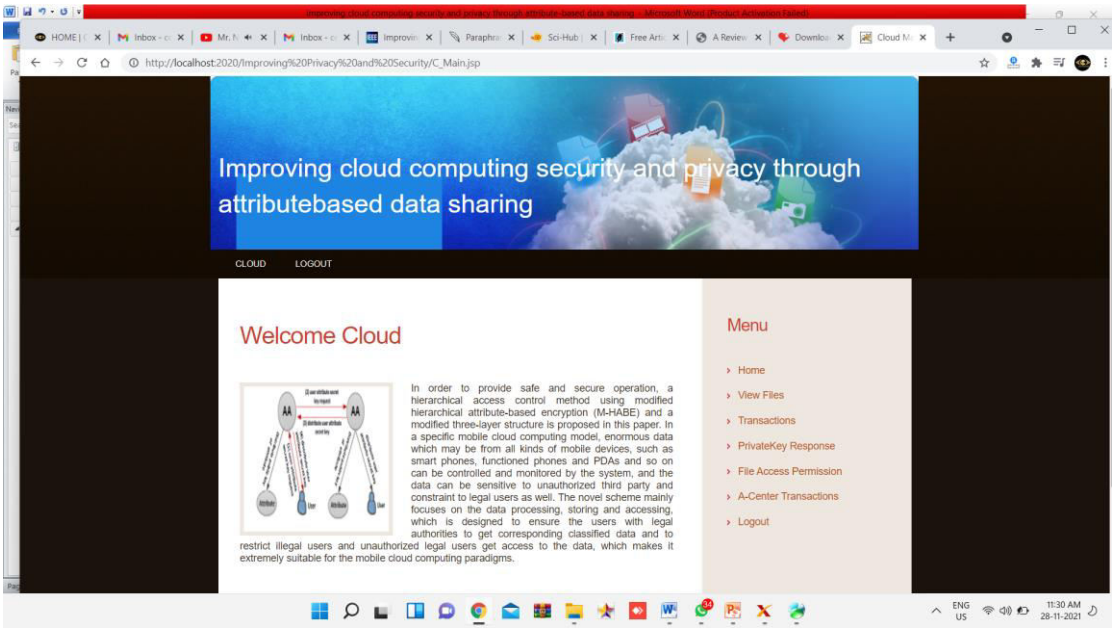

Fig 4.3 Cloud Main Page

5.CONCLUSION

We proposed a privateness keeping CP-ABE scheme in the widespread model. The introduced scheme has many blessings over the current schemes, such as steady dimension personal keys and brief ciphertexts. And in decryption, it solely wants 4 pairing computations. The proposed scheme achieves selective safety and anonymity in a top order group. In the popular model, we exhibit the safety of the proposed scheme is decreased to the decisional n-BDHE and the DL assumptions. Additionally, the proposed scheme helps authority verification with no privateness leakage. However, the added scheme solely helps "AND" coverage and depends on a susceptible safety model. How to assemble a robust invulnerable HP-CP-ABE scheme with greater bendy get right of entry to coverage is left for the future works.

REFERENCES

[1] P. P. Kumar, P. S. Kumar, and P. J. A. Alphonse, "Attribute based encryption in cloud computing: A survey, gap analysis, and future directions," J. Netw. Comput. Appl., vol. 108, pp. 37–52, 2018.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Applications Cryptographic Techn., May 2005, vol. LNCS 3494, 2015, pp. 457–473.

[3] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertextpolicy attribute-based encryption scheme with constant

ciphertext length," in Proc. 5th Int. Conf. Inf. Security Practice Experience, Apr. 2009, pp. 13– 23.

[4] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[5] M. Madejski, M. Johnson, and S. M. Bellovin, "A study of privacy settings errors in an online social network," in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on. IEEE, 2012, pp. 340–345.