Turkish Journal of Computer and Mathematics Education *Vol.9 No.3(2018),1270-1274*

Research Article

Using Attribute-Based Data Sharing to Improve Cloud Computing Security And Privacy

Mirza Moiz Baig[a], Umesh Samarth[b]. Rupesh Sharma[c], Purva Chandekar[d]

[a,b] Associate Professor, Department Of Information Technology, J D College of Engineering & Management, Nagpur
[c,d] Student, Department Of Information Technology, J D College of Engineering & Management, Nagpur

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.

Keywords: 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 a 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 and 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 something 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.

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 objective 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

In order to ensure data confidentiality and user privacy, an HP-CP-ABE framework with efficient authority identification is presented.

We devised an authority identification approach to save users from having to perform superfluous computations in the decryption algorithm by allowing them to verify whether or not they are permitted to decrypt.

Constant private key size independent of user attribute number is achieved by the suggested technique. It lowers the price of transmission and archiving.

The proposed method for achieving anonymity, which has been absent from most previous efforts, is demonstrated using a series of hybrid games that perform a compact security analysis.

3.1 Implementation

Data Owner

In this module, the data owner performs operations such as Upload Files, View Uploaded Files

User

In this module, he logs in by using his/her username and password. After Login receiver will perform operations like View Files, Search File on Cloud, Request Secret Key, View Secret Key Response, Request Certificate Permission, View Certificate Response

Certificate Authority

In this module, the sector can do following operations such as View Data Owners and Authorize, View Users and Authorize, View Files Meta Data, View Certificate Request and Permission, Secret Key Request and Generate

Cloud Server

The Cloud Server manages a server to provide data storage service and can also do the following operations such as View Files, Transactions, Secret Key Response, CA Authority Files, Download Request and Response, View File Score Results, View Time Delay Results , View Throughput Results

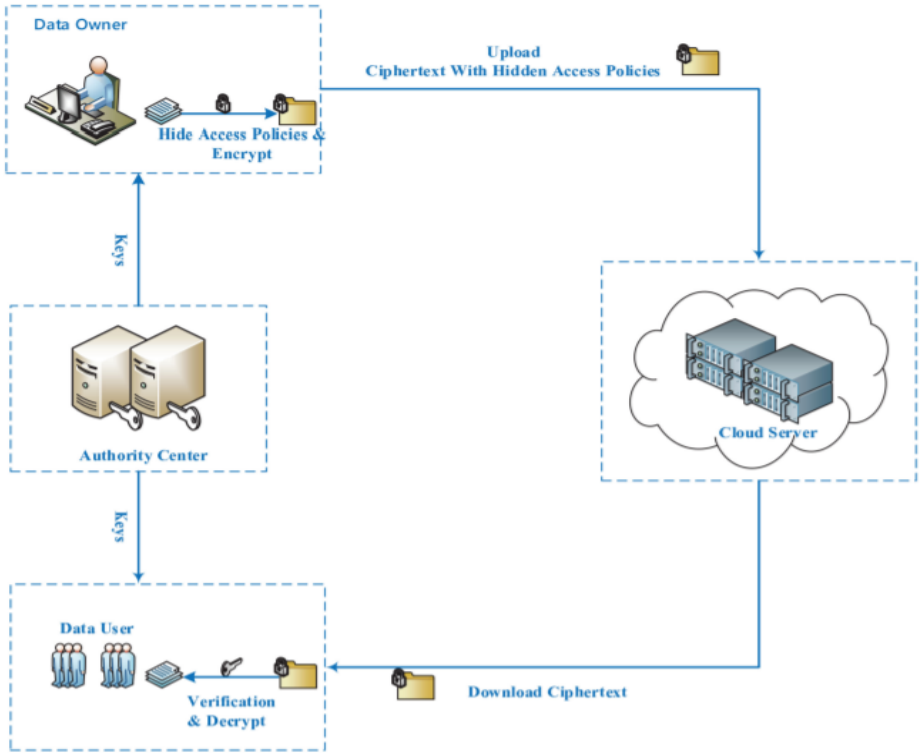

Fig 1: System Model

4. Results and Discussion

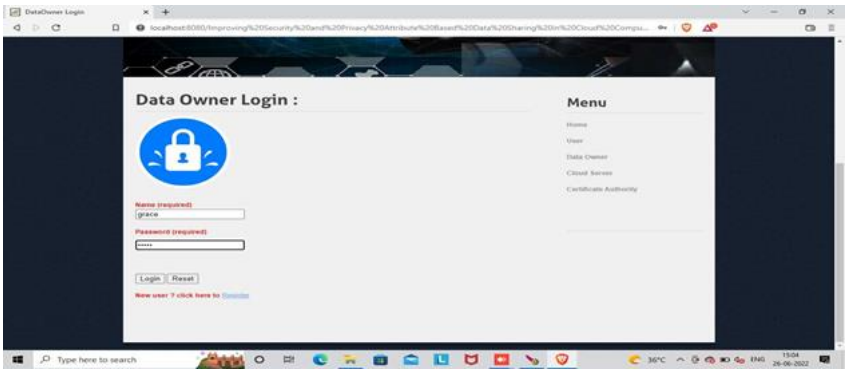

Fig 4.1: Data user Login form

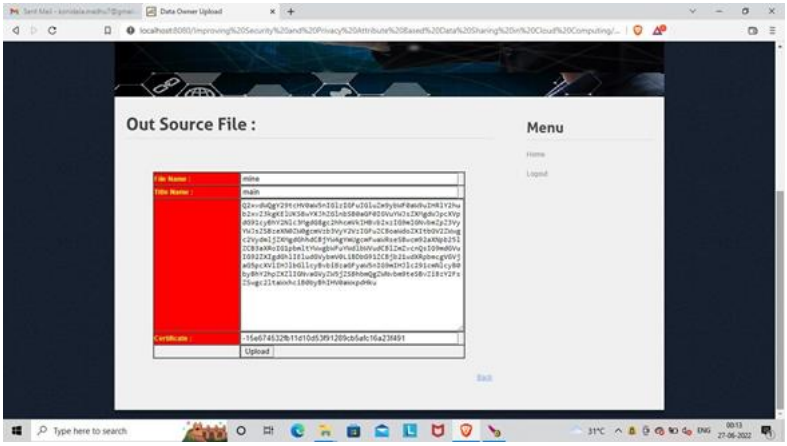

Fig 4.2: Encrypted Data

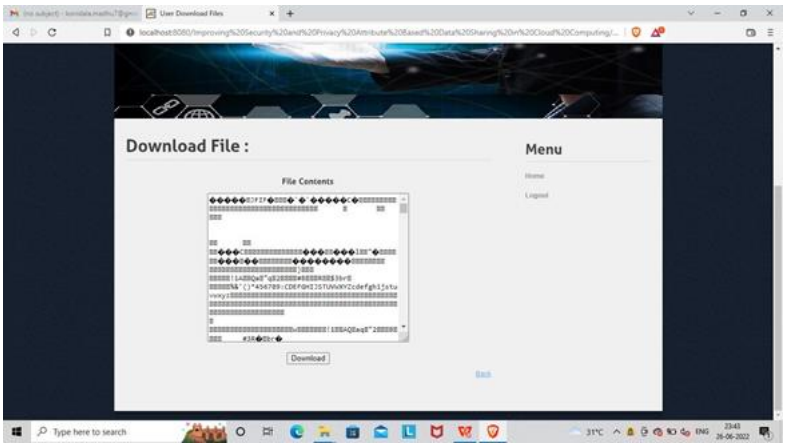

Fig 4.3: Decrypted Data

5.Conclusion

In the conventional model, we proposed a CP-ABE technique that protects user privacy. As compared to other methods, ours offers several advantages, such as private key constant size and short ciphertexts. And in decryption, only four pairing computations are required. Using the proposed method, a prime order group can be protected while maintaining anonymity. According to a conventional model, the suggested scheme's security is limited to the decisional NBDHE and DL assumptions. Furthermore, the suggested system allows for authority verification to be implemented while preserving user privacy. Although the new "AND" policy is supported, it relies on a weak security paradigm, making it vulnerable to attack. Future research is needed to figure out how to build a secure HP-CP-ABE system with a more flexible access policy.

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.