Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

CRYPTCLOUD+ : SECURE DATA ACCESS CONTROL OVER ENCRYPTED DATA

Mr. K. Mahanthi [1], Ms. Lavanya Naragani [2]

#1 Assistant Professor In The Department Of AI & IT at DVR & Dr HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District,A.P.

#2 MCA Student In The Department Of Computer Applications at DVR & Dr HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District,A.P.

Abstract— To propose an authority and revocable Crypt Cloud with white-box traceability and auditing to achieve Security guarantees should be provided –to protect the integrity of the data and the flexibility of access control over encrypted data. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is viewed as one of the most encouraging systems that might be utilized to verify the assurance of the administration. In any case, the utilization of CP-ABE may yield an inescapable security rupture which is known as the abuse of access certification (for example unscrambling rights), due to the inborn "win or bust" decoding highlight of CP-ABE. In this paper, we research the two fundamental instances of access qualification abuse: one is on the semi-believed specialist side, and the other is in favor of cloud client. To moderate the abuse, we propose the main responsible expert and revocable CP-ABE based distributed storage framework with white-box recognizability and reviewing, alluded to as CryptCloud+. We additionally present the security investigation and further exhibit the utility of our framework by means of trial.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

INTRODUCTION

A network or the Internet is referred to as a cloud. In other terms, the Cloud is something that exists in distant regions. Cloud services can be delivered across public and private networks, such as WAN, LAN, and VPN. Cloud-based applications include e-mail, conferencing, and customer relationship management (CRM). Cloud computing refers to the ability to remotely manipulate, configure, and access hardware and software resources. It provides data storage, infrastructure, and applications all across the internet. Important authorised clients have access to data that has been migrated any time, from any location, to the cloud. Encryption data before sending it to the web is one precautionary measure. None the less the maximum amount information sharing and handling as possible. This is often owing to the fact that before re-encoding, an information owner must first retrieve Scrambled data from cloud, is taken for distribution (takes without any consideration data. There are not any duplicates of the information in the Vicinity of the proprietor). A fine-grained admission command over scrambled data is advantageous in remote computing. CPABE (Cipher text-Policy Attribute-Based Encryption) [15] might be a good way to ensure information security, While also with fine-grained control. for instance , during a CP-ABE-based distributed storage framework, associations (e.g., a university like the University of Texas at San Antonio) and individuals (e.g., students, faculty members, and visiting researchers of the college) can first indicate an access strategy over expected cloud user qualities. Authorized cloud users are subsequently given access to the credentials (i.e., unscrambling keys) related to their characteristic sets (e.g., understudy job, employee job, or guest job), which may be used to gain access to the re-evaluated data. As a strong one-to-many encryption tool, CP-ABE not only provides a secure solution to guard information stored in the cloud, but it also allows for fine-grained access control. Existing CP-ABE-based distributed storage frameworks frequently overlook the likelihood of access certification abuse. as an example , a university might use a CPABE-based distributed storage framework to re-appropriate encoded understudy information to the cloud under certain conditions that are compliant with significant information sharing and protection regulations.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

LITERATURE REVIEW

Author: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano:We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent"so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanismas Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

Author:M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi:We identify and fill some gaps with regard to consistency (the extent to which false positives are produced) for public-key encryption with keyword search (PEKS). We define computational and statistical relaxations of the existing notion of perfect consistency, show that the scheme of [7] is computationally consistent, and provide a new scheme that is statistically consistent. We also provide a transform of an anonymous IBE scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally we suggest three extensions of the basic notions considered here, namely anonymous HIBE, public-key encryption with temporary keyword search, and identity-based encryption with keyword search.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

IMPLEMENTATION

Data Owner module:

Is an entity who encrypts its documents under an arbitrary access control policy and outsources them to the cloud. He/She considers the time of encrypting in generating the cipher texts. We should highlight that the data owner also encrypts his/her documents under his/her arbitrary access control policy. However, in this paper we concentrate on the encryption of the extracted keywords from documents.

Data User Module:

Is an entity who is looking for documents which contains an intended keyword, and are encrypted in a determined time interval. The time interval is arbitrarily selected by the data user.

Cloud Server Module:

Is an entity with powerful computation and storage resources. CS stores a massive amount of encrypted data, and receives the search tokens to look for the required documents on behalf of the data user. The cloud finds the relevant documents, and sends them back to the data user.

Trusted Third Party:

Is a fully trusted entity who receives each user's access tree, and generates their secret keys corresponding to his/her attributes set presented in his/her access tree. Then, the TTP sends back the users' credentials through a secure and authenticated channel.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

RELATED WORK

Cloud owners have complete control of their data and can download and erase it whenever they wish. They will assign some attribute set to their data while uploading it to the public cloud. A cloud user wishes to register their information with a cloud organisation so that they can access the data owner's information. Along with their designation, users desire to provide their personal information as characteristics. To get control over the data of the owner, the SemiTrusted Authority creates decryption keys. A user can manipulate cloud data in a variety of ways. Users in an organization's unique attribute set would be validated for each and every action. The admin would share these attributes with the cloud organization's permitted users. These characteristics will be saved in cloud-based policy files. If a user spills their unique decryption key to a malevolent user, data owners can track them down by submitting an audit request to an auditor, who will assess the request and determine who is responsible. By planning a responsible expert and revocable Crypt Cloud that supports white-box identifying and inspecting (referred to as Crypt Cloud+), we have tended to the test of certification spillage in a CP-ABE based distributed storage architecture. Crypt Cloud+, in particular, allows us to track and avoid malicious cloud clients (spilling certifications).

PROPOSED WORK

In existing system the CP-ABE may help us prevent security breach from outside attackers. But when an insider of the organization is suspected to commit the “crimes” related to the redistribution of decryption rights and the circulation of user information in plain format for illicit financial gains, how could we conclusively determine that the insider is guilty? Is it also possible for us to revoke the compromised access privileges? In addition to the above questions, we have one more which is related to key generation authority. A cloud user’s access credential (i.e., decryption key) is usually issued by a semi-trusted authority based on the attributes the user possesses. How could

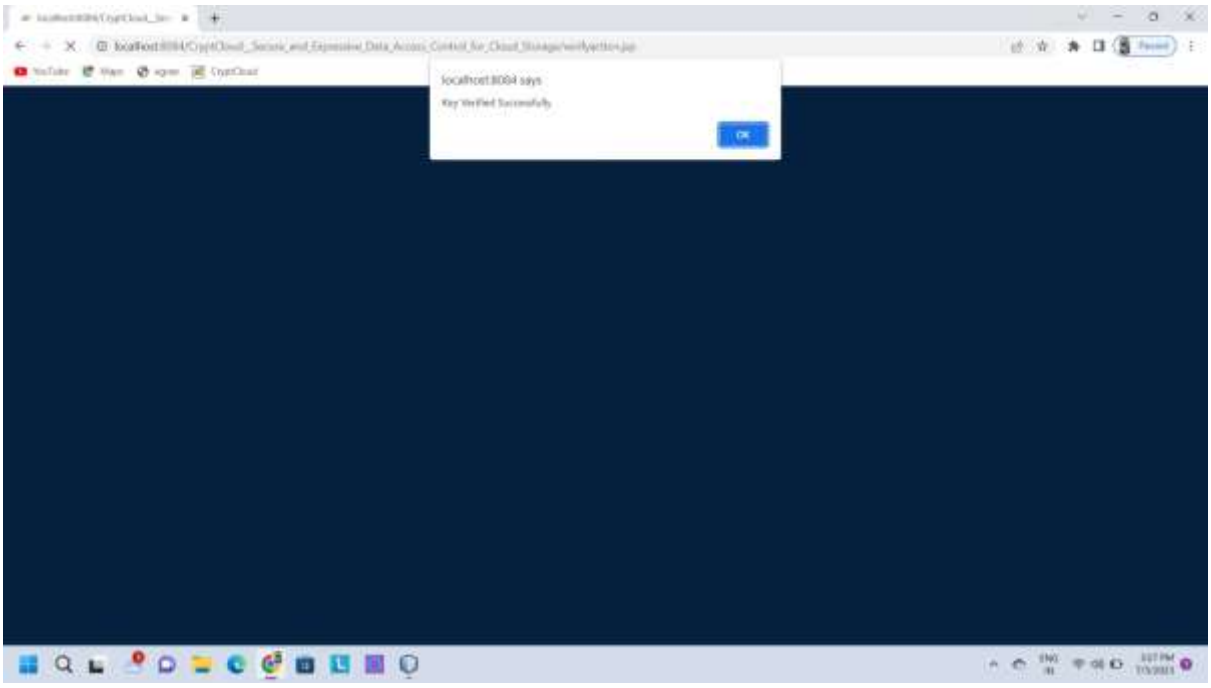
we guarantee that this particular authority will not (re-)distribute the generated access credentials to others.

Proposed System:

In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable Crypt Cloud which supports white-box traceability and auditing (referred to as Crypt Cloud+). This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, Crypt Cloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority.

SAMPLE SCREENSHOTS

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023



CONCLUSION

In this paper, we propose a challenge of credentialleakage in CP-ABE based cloud storage system by designingan accountable authority and revocable CryptCloud whichsupports white-box traceability and auditing (referred to asCryptCloud+). This is the first CP-ABE based

cloud storagesystem that simultaneously supports white-box traceability,accountable authority, auditing and effective revocation.Specifically, CryptCloud+ allows us to trace and revokemalicious cloud users (leaking credentials). Our approachcan be also used in the case where the users' credentials areredistributed by the semi-trusted authority.

We note that we may need black-box traceability, whichis a stronger notion (compared to white-box traceability),in CryptCloud. One of our future works is to consider theblack-box traceability and auditing.

REFERENCES

[1] Mazhar Ali, RevathiDhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya.Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

[2] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

[4] NuttapongAttrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

[5] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[6] MihirBellare and OdedGoldreich.On defining proofs of knowledge. In Advances in Cryptology-CRYPTO'92, pages 390–420. Springer, 1993.

[7] Dan Boneh and Xavier Boyen. Short signatures without random

oracles. In EUROCRYPT - 2004, pages 56–73, 2004.
[8] HongmingCai, BoyiXu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.
[9] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.
[10] Angelo De Caro and Vincenzo Iovino.jpbc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.
[11] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, andWenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.
[12] Zhangjie Fu, Fengxiao Huang, Xingming Sun, AthanasiosVasilakos, andChing-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.
[13] VipulGoyal. Reducing trust in the PKG in identity based cryptosystems. In Advances in Cryptology-CRYPTO 2007, pages 430–447. Springer, 2007.
[14] VipulGoyal, Steve Lu, AmitSahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008.
[15] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and DechaoQiu. Security of the internet of things: perspectives and challenges. Wireless Networks, 20(8):2481–2501, 2014.

.