A ES

https://doi.org/10.5281/zenodo.12726574

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

Fine-grained two-factor access control for web-based cloudcomputing services

D SNEHA, D SANKAR, VIJAYA BHASKAR MADGULA

Assistant Professor [1,2,3]

sneha.dharmavaram@gmail.com, shankar.dasari126@gmail.com, vijaya.bhaskar2010@gmail.com

Department of CSE, Sri Venkateswara Institute of Technology,

N.H 44, Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Keywords:

ABSTRACT

Through the use of the internet and a network of remote servers, organisations may now buy, rent, sell, or distribute software and other digital resources on demand. This model is known as cloud computing. Despite the many advantages of the new cloud computing paradigm, concerns about privacy and security for web-based cloud services persist. A system for controlling access to web-based cloud computing services that uses several factors of authentication is currently in development. The suggested authenticated access control system uses an attribute-based technique for controlling access; this mechanism necessitates the usage of a user secret key in addition to a trusted security key response. The login process is safeguarded by a system that requires a one-time password (OTP), and session keys are used to restrict the length of time a user may work. Since a user can't access the system without the OTP, secret key, and secret key response, the procedure enhances the system's security, especially in situations when several users utilise the same machine for web-based cloud services. Additionally, the system's attribute-based administration enables the cloud server to restrict access to individuals who possess similar attributes, all while ensuring user privacy. The user's predicate compliance is all the information the cloud server has; it is unaware of the user's identity. User policies and traits are saved in the cloud. Because the data is encrypted and only the user has the key, no one in the cloud can see the user's data. Among the most important concepts are: session keys, cloud storage, encryption, key response, encryption key, and access control.

A ES

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726574

1. INTRODUCTION

- Businesses may now purchase, rent, sell, or distribute software and other digital resources on the internet as a service using cloud computing, which is a virtual host computer system. Since it is now a virtual system, it is independent of the server or the amount of actual computers. Cloud computing has several uses, including medical information systems, large data management, data storage, and sharing. The business software and user data are kept on distant servers, and end users access these programmes using web browsers, thin clients, or mobile apps. Accessibility, lower prices and capital expenditures, improved operational efficiency, scalability, flexibility, and quick time to market are just a few of the many advantages of web-based cloud computing services. Cloud computing is a new paradigm that offers many benefits, but there are also certain worries about privacy and security, particularly with web-based cloud services. User authentication is now an essential part of any cloud system since sensitive data may be kept there for easy access or sharing, and because authorised users can use the cloud for a variety of apps and services. Any time a user wants to utilise the cloud services or get to their private data kept there, they have to check in. The old-fashioned approach that relies on accounts and passwords has two major flaws. To begin, the standard method of authentication that relies on accounts and passwords does not protect users' privacy. We must take into account the fact that privacy is a crucial aspect in cloud computing systems, however. Second, having many individuals use the same computer is very normal. Installing spyware to collect the login password from the web browser could be a simple task for hackers. The first issue may be effectively addressed by using attribute-based access control, a newly suggested methodology for access control. Furthermore, it creates access control rules depending on various requester, environment, or data object criteria and offers anonymous authentication. The authority issues a user secret key to each user in an attribute-based access control system1. In actuality, the user's secret key is kept inside the computer. Considering the second issue with web-based services, it is very uncommon for several users to use a single computer, particularly in larger organisations. Here are two examples that illustrate my point:

  - In a hospital ,computers are shared by different staff. Dr. Alice uses the computer

  in room A when she is on duty in the daytime, while Dr. Bob uses the same computer in the same room when he is on duty at night.

  - In a university, computers in the undergraduate lab are usually shared by different students. In these cases, user secret keys could be easily stolen or used by an unauthorized party. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares.

- Using two-factor authentication (2FA) is a safer option. Many online banking services use two-factor authentication. A one-time password display device is also necessary for those who do not have a login and password. A user's mobile phone may be necessary for some systems; while logging in, a one-time password may be delivered to the phone via text message. Users will feel more secure logging into web-based e-banking services from shared computers when 2FA is in place. The same logic applies to why two-factor authentication (2FA) is the way to go for web-based cloud service security.

A ES
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726574

1.1 Our Contribution

2. Using a small security device, we provide a protocol for web-based cloud computing services that uses two-factor authentication with fine-grained control. Here are the features that this gadget possesses:
(1) it is capable of computing a few simple algorithms, such as hashing and exponentiation
(2) It is believed that no one can get into it and acquire the secret information contained within since it is tamper proof. Our protocol adds two-factor authentication (2FA) to this gadget. To begin, you'll need the user's secret key, which is often kept inside the machine itself. To further ensure the user's identity while using the cloud, the security device must be linked to the computer (for instance, via USB). Only if the person has both objects will he be permitted entry. In addition, the user is not allowed to utilise his secret key on someone else's device in order to get access. Our protocol allows for attribute-based access at granular levels, giving the system a lot of leeway to adapt its access regulations to various situations. This is all while the user's privacy is protected. The cloud service provider is unaware of the user's true identity; all it knows is that they have a certain property that is necessary. In order to demonstrate that our system is feasible, we model the prototype of the protocol. We shall examine a number of relevant works that touch on our idea in the section that follows.

3. RELATED WORK

We review some related works including attribute-based cryptosystems and accesscontrol with security device in this section.

3.1 Attribute-Based Cryptosystem

4. The foundation of an attribute-based cryptosystem is attribute-based encryption (ABE). ABE allows for granular control over who may access encrypted data by associating characteristics with private keys and ciphertexts and implementing access controls. The encryptor specifies the access policy that the decryptor (and their set of characteristics) must meet in order to decipher the cypher text, and CP-ABE provides a scalable method of data encryption within this framework. This means that according to the policy that was set up in advance, various people may decrypt different types of data. Because of this, users may lose faith in the storage server's ability to keep sensitive information safe. Along with encrypted data in the cloud storage service, authorised access is another concern. When it comes to controlling who has access to what in the cloud, ABE is just as useful as any encryption system. as a means of authentication, the server in the cloud may encrypt an unsolicited communication using the policy for access and then request that the user decode it. To use the cloud computing service, a user must be able to decipher the cypher text, which indicates that their attribute set meets the policy requirements. Along with ABE, attribute-based signature (ABS) is another cryptographic primitive in the attribute-based cryptosystem. Users have granular control over their identifying information when signing messages using an ABS method. Attribute private keys are obtained by users from attribute authorities in an ABS system. Later on, they'll be able to sign messages for any predicate that their characteristics satisfy. The validity of the signature convinces the verifier that the signer's traits meet the signing predicate. There is also an anonymity around the signer. Thanks to this, anonymous attribute-based access control may be effectively implemented. A new attribute-based access control method, suggested by Yuen et al., might be seen as an interactive version of ABS.

A ES
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726574

4.1 Access Control with Security Device

Security Mediated Cryptosystem

The first implementation of mediated cryptography it as a way to make it possible to revoke public keys instantly. Using a third party intermediary in every transaction is the core principle of mediated cryptography. An SEM, short for "Security Mediator," is an online mediator that allows for the management of security capabilities. It will be unable to conduct any transactions using the public key if the SEM refuses to comply. A form of SEM that is based on attributes was recently suggested in. "Security mediated certificate less" (SMC) cryptography is an evolution of the original SEM concept. A person's identity, public key, and secret key all work together in an SMC system. The combination of the secret key and the SEM is necessary for the signing or decryption algorithm. The user's public key and associated identification are necessary components of the technique used for signature verification or encryption. The authority in charge of handling user revocation also refuses to cooperate with any revoked user, as the SEM is under their control. This means that deactivated accounts can't create signatures or decode encrypted messages. It should be noted that our notion differs from SMC. Addressing the revocation issue is SMC's primary objective. Therefore, the authority controls the SME. To rephrase, each time a signature is needed or a cypher text is deciphered, the authority must be present online. The user is not anonymous in SMC. Whilein our system, the security device is controlled by the user. Anonymity is alsopreserved.

Key-Insulated Cryptosystem In [10], key-insulated cryptography was first proposed. Safeguarding long-term keys in a device that is both physically and computationally constrained was the basic premise of key-insulated security. Users store short-term secret keys on a robust but unprotected gadget that performs cryptographic calculations. The user and the base interact to renew the short-term secrets at periodic intervals, while the public key stays the same throughout the system's lifespan. When a new time period begins, the gadget provides the user with a partial secret key. The user may renew the secret key for the current time period by combining this partial key with the secret key for the prior period. A key-insulated cryptosystem differs from our approach in that it mandates regular key updates for all users. In order to update the keys, the security device is needed. The signing or decryption method no longer needs the device within the same time period after the key has been changed. Although our idea necessitates the security device each time the user attempts to access the system. Furthermore, there isno key updating required in our system.

5. PROPOSED SYSTEM

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726574

Figure 1 User Key Generation Process

Figure1 shows the user key generationprocess, firstly user has to request for devicefrom the trustee if the attributes matches the requirements then trustee will issue the security device it will be the first level of access to download file in cloud and next user has to request for secret key from the attribute issuing authority, if attributes matches with the requirements then the attribute issuing authority will issue the secret key it will be the second level of access.

Figure 2 User Access Authentication Process

A simplistic approach to accomplishing our objective would be to use a standard ABS and only divide the user's secret key into two halves. While the user retains one copy on their computer, the

A ES
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726574

security device receives the second copy to begin with. Due diligence is required since, unlike standard ABS, which ensures that the scheme's security is unaffected by the disclosure of even a partial secret key, an attacker may have compromised one of the elements in two-factor authentication. Additionally, since the security device is not meant to be powerful, the splitting should be done in such a manner that the user's computer should be mostly responsible for computing. On purpose, we've built our system in a different way. We will not divide the secret key in half. We choose to include some more distinct data saved instead. in the security device. The authentication process requires this piece of informationtogether with the user secret key

5.1 Entities

Our system consists of the following entities:

- **Trustee:** It is responsible for generating allsystem parameters and initializes the security device.
- **Attribute-issuing Authority:** It is responsible to generate user secret key for each user according to their attributes.
- **User:** It is the player that makes authentication with the cloud server. Each user has secret key issued by attribute- issuing authority and security device initialized by the trustee.
- **Cloud Service Provider:** It provides services to anonymous authorized users. It interacts with the user during the authentication process.

6. CONCLUSION

7. We have introduced a novel two-factor authentication solution for web-based cloud computing services in this work. It incorporates both the user's private key and a lightweight security device. In order to protect user privacy and allow the cloud server to limit access to users with the same set of characteristics, the proposed two-factor authentication (2FA) access control system was developed using the attribute-based access control method. According to the results of the thorough security study, the suggested two-factor authentication system meets all of the security criteria.

8. REFERENCES

CIt was written by Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhaohr. Cloud storage services that are widely used have security issues. article published in 2013 by IEEE Pervasive Computing, volume 12, issue 4, pages 50–57.
[2] inX. Huang, Y. Xiang, J. K. Liu, Q. H. Vu, and J. Baek. The smart grid's big data information management system built on secure cloud computing. 2015. IEEE Transactions on Cloud Computing, 3(2), 233-244.

Three authors: J. Bethencourt, A. Sahai, and B. Waters. A policy-based encryption method for ciphertexts. On pages 323–334 of the IEEE Symposium on Security and Privacy. Computer Society

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726574

of the IEEE, 2007.
Han, J., Susilo, W., Mu, Y., and Yan, J. (2018). Secure attribute-based decentralised key-policy encryption that maintains privacy. published in 2012 by IEEE Transactions on Parallel Distributed Systems, volume 23, issue 11, pages 2150–1572.
Secure data exchange in smart grid based on attributes with concealed policies [5] JHur.2013. In IEEE Transactions on Parallel Distributed Systems, 24(11): 2171–2180.
k-times attribute-based anonymous access control for cloud computing [6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, J. Zhou. computer science, 2015, vol. 64, no. 9, pp. 2595–2608.
Written by D. Boneh, X. Ding, and G. Tsudik [7]. Fine- grained control of security capabilities. , 2004. ACM Transactions on Internet Technology, 4(1), 60–82.Authors: X. Wang, M. H. Au, J. K. Liu, S. Yiu, Z. L. Jiang, and Y. Chen. Cryptically sound

text-policy attribute-based encryption using a security mediator. The paper may be found on pages 274-289 in the Lecture Notes in Computer Science, volume 8958, ICICS '14. Publisher: Springer, 2014.
[8] G. Nieto, C. Boyd, and S. S. M. Chow. Mediated cryptography without certificates for security purposes. Pages 508–524 of the Lecture Notes in Computer Science volume 3958, devoted to public key cryptography. Press, 2006.
[10]Written by Y. Dodis, J. Katz, S. Xu, and M. Yung. Privacy-preserving public key cryptosystem with no key exposure. On pages 65–82 of the EUROCRYPT volume 2332 of the CSE lecture notes.In 2002, Springer published.