

FINE GRAINED ACCESS CONTROL WITH TWO-FACTORS AUTHENTICATION FOR CLOUD COMPUTING PLATFORM

Ms. Lavanya B¹, Deepa T², Kaviya S³, Malini R⁴, Dhanusri E⁵

^{1,2,3,4} UG Students, Computer Science and Engineering Bharathiyar Institute of Engineering for Women (Autonomous), Salem, Tamilnadu, India

⁵ Assistant Professor, Computer Science and Engineering & Bharathiyar Institute of Engineering for Women (Autonomous), Salem, Tamilnadu, India

Abstract: In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

1. INTRODUCTION

Sometimes referred to as computer security information technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses.

They are responsible for keeping all of the technology within the company secure from

malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

The act of providing trust of the information, that the Confidentiality, Integrity and Availability (CIA) of the information are not violated. E.g., ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction or physical theft. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

2. PROBLEM STATEMENT

The performance of the proposed system "Strengthening Cloud Security: Fine-Grained Access Control with Two-Factor Authentication for Cloud Computing Platforms" is analyzed based on security efficiency, response time, and system reliability when implemented on cloud environments such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform. Authentication Efficiency

The system uses Two-Factor Authentication (2FA) which includes:

- Password verification
- OTP verification-This reduces the chances of unauthorized access. Even if a password is compromised, the attacker cannot log in without the OTP.
- Therefore, the authentication success rate for legitimate users is high while blocking unauthorized attempts. Access Control Accuracy
- The Fine-Grained Access Control mechanism assigns permissions based on user roles (Admin, Manager, User).

3. LITERATURE REVIEW

A literature review is an account of what has been published on a topic by accredited scholars and researchers. Occasionally you will be asked to write one as a separate assignment, but more often it is part of the introduction to an essay, research report, or thesis. In writing the literature review, your purpose is

to convey to your reader what knowledge and ideas have been established on a topic, and what their strengths and weaknesses are. As a piece of writing, the literature review must be defined by a guiding concept (e.g., your research objective, the problem or issue you are discussing or your argumentative thesis). It is not just a descriptive list of the material available, or a set of summaries

Besides enlarging your knowledge about the topic, writing a literature review lets you gain and demonstrate skills in two areas

1. **INFORMATION SEEKING:** the ability to scan the literature efficiently, using manual or computerized methods, to identify a set of useful articles and books
2. **CRITICAL APPRAISAL:** the ability to apply principles of analysis to identify unbiased and valid studies.

4. PROPOSED METHODOLOGY

4.1. System Overview

The proposed system provides secure data access in cloud environments by integrating fine-grained access control mechanisms with two-factor authentication (2FA).

The methodology ensures that:

- Only authorized users can access cloud resources.
- Access permissions are controlled using attribute-based policies.
- A second authentication factor improves security against unauthorized access.

The system consists of four main entities:

1. Data Owner
2. Cloud Server
3. Attribute Authority
4. Data User

4.2. System Architecture

- Uploads files to the cloud.
- Defines fine-grained access policies.
- Encrypts data before storing it in the cloud.

Example policy:

(Department = HR AND Role = Manager)

Only users with those attributes can access the file.

4.3. Attribute Authority (AA)

- Issues attribute-based secret keys to users.
- Verifies user identity.
- Manages user attributes such as:
 - Department
 - Role
 - Organization level

5. RESULT AND DISCUSSION

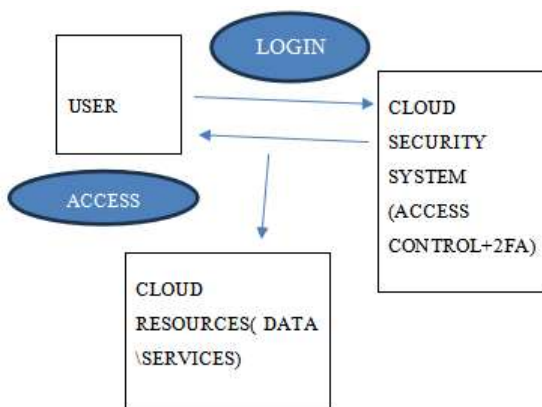
5.1 Implementation Result

The proposed system was implemented to evaluate the effectiveness of fine-grained access control combined with two-factor authentication (2FA) in a cloud computing environment. The system includes modules such as user registration, authentication, attribute-based key generation, data encryption, cloud storage, and secure data access.

During implementation, the following operations were successfully performed:

1. **User Registration and Attribute Assignment**
Users were registered in the system and assigned attributes such as role, department, and designation by the Attribute Authority. These attributes determine the access privileges of each user.
2. **Two-Factor Authentication Process**
The login process required users to enter their username and password as the first authentication factor. After successful password verification, a One-Time Password (OTP) was generated and sent to the user's registered mobile number or email. Only after entering the correct OTP could the user access the system.
3. **Data Encryption and Upload**
Data owners defined fine-grained access policies and encrypted the data using an attribute-based encryption technique before uploading it to the cloud server. The encrypted data was stored securely in the cloud storage system.
4. **Access Control Verification**
When a user requested access to a file, the system verified whether the user's attributes satisfied the access policy defined by the data owner. If the attributes matched the policy, the user was allowed to download and decrypt the file.
5. **Secure Data Decryption**
Authorized users were able to decrypt and access the data successfully using their attribute-based keys. Unauthorized users were denied access even if they attempted to retrieve the encrypted data.

6. SAMPLE OUTPUT



7.CONCLUSION

In this paper, we have presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, we demonstrated that the construction is “feasible”. We leave as future work to further improve the efficiency while keeping all nice features of the system.

8. ACKNOWLEDGEMENT

The authors express their sincere thanks to the Department of Computer Science and Engineering, Bharathiyar Institute of Engineering for Women, for their continuous support and guidance in completing this research work successfully.

9. REFERENCES

- [1] M. H. Au and A. Kapadia. PERM: practical reputation-based blacklisting without TTPS. In T. Yu, G. Danezis, and V. D. Gligor, editors, *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, pages 929– 940. ACM, 2012.
- [2] M. H. Au, A. Kapadia, and W. Susilo. Blacr: Ttp-free blacklistable anonymous credentials with reputation. In *NDSS*. The Internet Society, 2012.
- [3] M. H. Au, W. Susilo, and Y. Mu. Constant-Size Dynamic k -TAA. In *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 111–125. Springer, 2006.
- [4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of smart grid. *IEEE T. Cloud Computing*, 3(2):233–244, 2015.
- [5] M. Bellare and O. Goldreich. On defining proofs of knowledge.
- [6] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334. IEEE Computer Society, 2007.
- [7] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In Franklin [19], pages 41–55.
- [8] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. *ACM Trans. Internet Techn.*, 4(1):60–82, 2004.
- [9] J. Camenisch. *Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem*. PhD thesis, ETH Zurich,
- [10] J. Camenisch, M. Dubovitskaya, and G. Neven. Oblivious transfer with access control. In E. Al-Shaer, S. Jha, and A. D. Keromytis, editors,
- [11] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In S. Cimato, C. Galdi, and G. Persiano, editors, pages 268–289. Springer, 2002.
- [12] J. Camenisch and A. Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. In Franklin [19], pages 56–72.
- [13] Y. Chen, Z. L. Jiang, S. Yiu, J. K. Liu, M. H. Au, and X. Wang. Fully secure ciphertext-policy attribute based encryption with security mediator. In *ICICS '14*, volume 8958 of *Lecture Notes in Computer Science*, pages 274–289. Springer, 2014.
- [14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto. Security-mediated certificateless cryptography. In *Public Key Cryptography*, volume 3958.