Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 1, January - 2018

TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage

Snehal [1], Priyanka[2], Apurva[3],Gayatri[4], Prof. Ashwini k. Bhavsar[5]

Department of Computer Engineering, PCP, Pune, Maharashtra, India, snehalp2000@gmail.com,
Department of Computer Engineering, PCP, Pune, Maharashtra, India, jadhavpriyanka8482@gmail.com
Department of Computer Engineering, PCP, Pune, Maharashtra, India, pachghare.gayatri@gmail.com
Department of Computer Engineering, PCP, Pune, Maharashtra, India, apurvasherkhane2000@gmail.com
Department of Computer Engineering, PCP, Pune, Maharashtra, India, ashwini.k.bhavsar@gmail.com

Abstract — Attribute-based Encryption (ABE) is regarded as a promising cryptographic conducting tool to guarantee data owners' direct control over their data in public cloud storage. The earlier ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on both security and performance. Subsequently, some multi-authority schemes are proposed, in which multiple authorities separately maintain disjoint attribute subsets. However, the single-point bottleneck problem remains unsolved. In this paper, from another perspective, we conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (t, n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. Furthermore, by efficiently combining the traditional multi-authority scheme with TMACS, we construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Keywords **-** CP-ABE, (*t; n*) threshold secret sharing, multi-authority, public cloud storage, access control

I. INTRODUCTION

Despite many advantages of cloud storage, there still remain various challenging obstacles, among which, privacy and security of users' data have become major issues, especially in public cloud storage. Traditionally, a data owner stores his/her data in trusted servers, which are generally controlled by a fully trusted administrator. However, in public cloud storage systems, the cloud is usually maintained and managed by a semi-trusted third party (the cloud provider). Data is no longer in data owner's trusted domains and the data owner cannot trust on the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a critical challenging issue in public cloud storage, in which traditional security technologies cannot be directly applied.

Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds for it can guarantee data owners' direct control over their data and provide a fine-grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories: Key- Policy Attribute-based Encryption (KP-ABE), such as and Cipher text-Policy Attribute-based Encryption (CPABE), decrypt keys are associated with access structures while cipher text are only labeled with special attribute sets.

In this paper, we propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute.

In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (*t*, *n*) threshold secret sharing guarantees that the master key cannot be obtained by any authority alone. TMACS is not only verifiable secure when less than *t* authorities are compromised, but also robust when no less than *t* authorities are alive in the system.

II.LITERATURE SURVEY

Data confidentiality and access control are two basic security requirements for outsourced data in cloud computing. Sometime, when we emphasize more on security of data, we forget about performance of systems (DO, CSP, users). For example, to secure data, we sometime use too many keys. We know that keys are confidential, so there is need to secure and maintain these keys which are additional work. These additional works affect the performance of the system. So, it is desirable to reduce no of keys. So, there is need a scheme that provides not only data security but also maintain the performance. Many schemes are suggested to meet these requirements.

The scheme proposed is the group-key scheme. In group-key scheme, there is a single key corresponding to each group of users for decryption process and all users of the group know that key. Here, number of keys is reduced but there is a problem of collusion attack of CSP and a user because a single malicious user can leak whole data of the group to CSP. We know that CSP is not trusted party. It can use data owner's data for its commercial benefits.

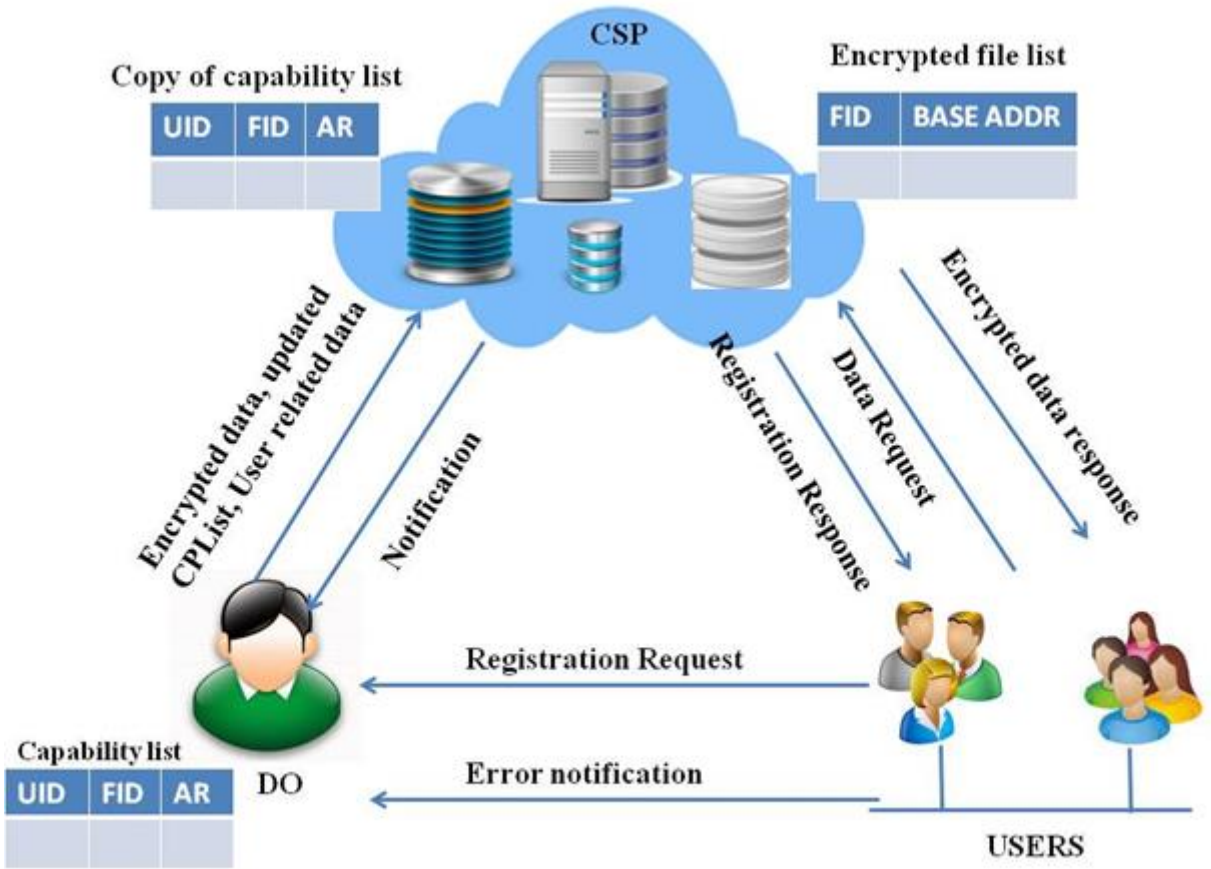
The scheme proposed in [4] tried to achieve data confidentiality and access control. In this scheme, data are encrypted by symmetric keys and symmetric keys are known only to data owner and corresponding data users. The encrypted data are stored at CSP. CSP can't see data stored at it as data are encrypted. Data are further encrypted by one time secrete session-key shared between CSP and user by the modified Diffie-Hellman protocol to protect data from outsiders during the transmission between CSP and user. This scheme no doubt provides whole data security but there is associated a key corresponding to each user and users may be large in number in some applications. So, number of keys may increase. Hence, increases the maintenance and security concerns of keys

Communication model of the proposed scheme somehow matches with it [4] but proposed scheme is more secure and reduces number of keys. The proposed scheme is useful for those applications where works are done in team and group such as in software industries. You may think proposed scheme has limited applications but it is not as such. It is applicable all where you can group users on some basis and can apply threshold cryptography technique. Such as software and hardware industries, institutes, banks and medicals fields. There is provision of hierarchy of access in this scheme which makes this scheme more useful and realistic. For Example, an university has vice-chancellor, hods, teachers, clerklier-staff and students. Each one has different level of access right.

III .PROPOSED SYSTEM

We propose a robust and verified threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key used to generate attribute private keys, we introduce (t, n) threshold secret sharing into our scheme to share the secret key among authorities.

IV.SYSTEM DESIGN



V ADVANTAGES

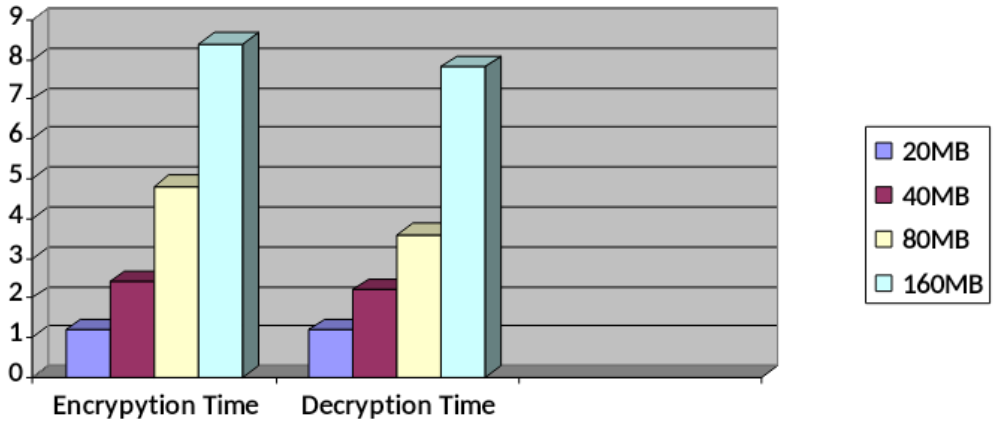
- Access control scheme is robust and secure

- Threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any *t* authorities.

VI RESULT

File size	Encryption time	Decryption time
20MB	1.2	1.2
40MB	2.4	2.2
80MB	4.8	3.6
160MB	8.4	7.8

Table I: Performance of File Size with Time



VI CONCLUSION

In this paper, we propose a new threshold multi-authority CP-ABE access control scheme, named TMACS, in public cloud storage, in which all *AA*s jointly manage the whole attribute set and share the master key α. Taking advantage of (*t*, *n*) threshold secret sharing, by interacting with any *t AA*s, a legal user can generate his/her secret key. Thus, TMACS avoids any one *AA* being a single-point bottleneck on both security and performance. The analysis results show that our access control scheme is robust and secure. We can easily find appropriate values of (*t*, *n*) to make TMACS not only secure when less than *t* authorities are compromised, but also robust when no less than *t* authorities are alive in the system.

VII REFRENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology*, vol. 53, no. 6, p. 50, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Proceedings of the 14th Financial Cryptography and Data Security*. Springer, 2010, pp. 136–149.

[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2005, pp. 457–473.

[5] R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2014, pp. 195–203.

[6] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2010, pp. 62–91.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 89–98.

[8] N. Attrapadung, B. Libert, and E. Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts," in *Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography*. Springer, 2011, pp. 90–108.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of IEEE Symposium on Security and Privacy*. IEEE, 2007, pp. 321–334.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography*. Springer, 2011, pp. 53–70.z