Secure Box - Encrypted cloud storage solution

COMPUTER & INFORMATION SCIENCE & ENGINEERING

UF Herbert Wertheim College of Engineering UNIVERSITY of FLORIDA

Sunny Dhama

Abstract

There are numerous cloud storage and security options, and because they all employ unique strategies, they offer varying degrees of protection. In this poster, we look at examples of each type of solution and try to come up with a solution that would use cloud storage options and industry-standard encryption methods. Our research shows how we could use Attribute-Based Encryption (ABE) schemes in conjunction with RSA digital signing to securely store data and files on the cloud. We also implemented a prototype to test our hypothesis.

Introduction

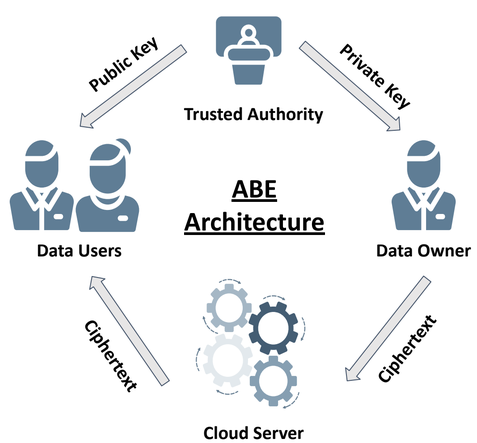
In this study, we investigated various Attribute-Based Encryption (ABE) schemes, including Multi-Authority-based Weighted ABE (MA-WABE) and Hierarchical ABE, as well as blowfish and homographic encryption methods. In order to increase reliability and performance, we have discovered that using digital signatures with RSA and MA-WABE is a viable option. According to the study, for role-based access control, hierarchical ABE should be used in addition to standard ABE. In order to compare the ABE and RSA methods, the prototype also incorporates a digital signature with RSA encryption. To improve cloud security, a hybrid of homographic and blowfish encryption methods was also investigated. While developing this application, current threats and cloud attacks were tested against our infrastructure. Malware injection and wrapping attacks were tested on the prototype and the encryption techniques (ABE with RSA digital signatures) were resilient to them.

Methodology

The implementation of secure cloud storage solution was conducted in two phases. In phase one we conducted a multitude of tests to select the combination of encryption algorithms to use on our cloud storage solution. Through intensive testing we chose ABE with RSA digital signatures as it provided consistent results, both in terms of encryption speed and handling of large files. Fig. 1 shows the methods used and advantages of each methods tested for the implementation.

Encryption technique	Method	Advantage
AES	Approach based on key length output	Secure cloud data message transaction between the client and the server
AES+ECC	A multilevel schema where ECC is used to encrypt AES keys	Ensures authentication, confidentiality and integrity
ABE + RSA	Uses attribute based encryption and digital RSA signatures	Ensure low cost and high security level for large files
Blowfish + HA	Encrypt the input text firstly with HA then BE	Enhance cloud security (high security level)
Blowfish + clustering	Combine blowfish with clustering techniques (K-method)	Ensures high security level

Fig 1 Comparison of different encryption algorithms



Steps that were performed to achieve ABE encryption are as follows:

Setup: The authority produces the public parameter Public Key (PK) and Master Secret Key (MSK) using no-zero random values.

KeyGeneration: Authority produces the user's secret key (S) for every user.

Encryption: This algorithm produces the ciphertext. The message (M) is encrypted using PK and set of attributes used as an identity by data owner.

Decryption: Data user decrypts the message from ciphertext using secret key S. S generated with the identity (AU) and ciphertext is generated with the identity.

Results

We developed an cloud storage solutions is fast and robust. Fig 2 shows the encryption, description and key generation time for the hybrid encryption approach.

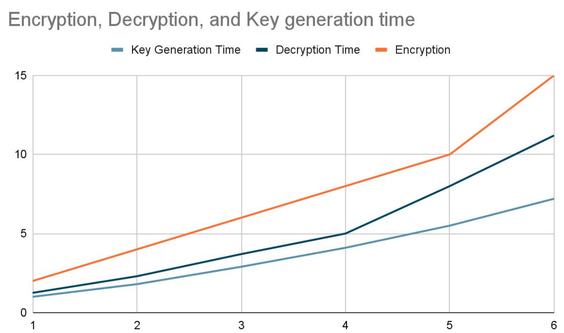
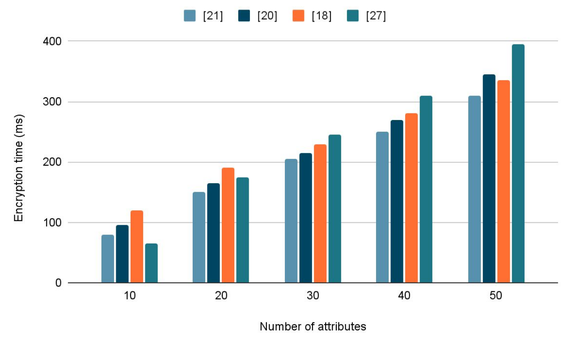


Fig 2 Key Generation, Encryption and Decryption Time analysis

Execution time also depends upon the number of attributes used in the ABE encryption algorithm. We choose the most optimal based upon the security offered and full process execution time.



ABE used with RSA digital signatures was implemented with resilience to cloud attacks in mind, this approach mitigates most of the well known attacks on cloud storages. Few of the attacks like DoS and Injection of the cloud malware were tested using Kali Linux.

Conclusion

ABE is a widely used encryption method for restricting access in cloud computing. The main benefits of ABE are the spread of key strengths and access to more powerful encryption for users. In the paradigm of secure encryption techniques for cloud storage, the analysis results show that our file encryption is robust and secure. Furthermore, based on efficiently combining the traditional ABE scheme, we also construct a hybrid scheme that is more suitable for the real scenario with RSA digital signatures. This enhanced scheme addresses not only attributes coming from ABE but also security and system-level robustness.

Acknowledgement

Prof. Patrick Traynor, John H. and Mary Lou Dasburg Preeminent Chair in Engineering and Associate Chair for Research