Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 4 (2016) 12 - 16. Submitted 29/10/2016. Published 12/11/2016

POLYNOMIAL INTERPOLATION BASED SPACE EFFICIENT VERIFIABLE SECRET SHARING DATA ANALYSIS

[1]G.Sasikala, [2]K.Anbumathi,
[1]M.Phil Scholar, Dept of Computer Science, Bharathiyar Arts and Science College for Women, Deviyakurichi,
[2]Assistant professor, Dept of Computer Science, Bharathiyar Arts and Science College for Women, Deviyakurichi.

Abstract:

Preserving data confidentiality in clouds is a key issue. Secret Sharing a cryptographic primitive for the distribution of a secret among a group of n participants designed so that only subsets of shareholders of cardinality 0 < t n are allowed to reconstruct the secret by pooling their shares can help mitigating and minimizing the problem. A desirable feature of Secret Sharing schemes is swindler detection. The capability to identify one or more malicious shareholders trying to restructure the secret by obtaining legal shares from the other shareholders while providing them with counterfeit shares. Verifiable Secret Sharing schemes solve this predicament by allowing shareholders verifying the others' shares. We present new verification algorithms provided that arbitrary secret sharing schemes with cheater detection capabilities and prove their space efficiency with regard to other schemes appeared in the literature. Our schemes the Exponentiation Polynomial Root Problem (EPRP), which is believed to be NP-Intermediate and therefore difficult.

Keywords: Exponentiation Polynomial Root Problem, security, cryptographic.

1. INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or individual devices to switch applications. In cloud computing the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet" so the turn of phrase cloud computing income "a type of Internet-based computing" where different services -- such as servers, storage space and applications -- are delivered to an organization's computers and devices through the Internet. Cloud computing is equivalent to grid computing a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine. secret Sharing deals with the problem of securely distributing confidential information among a certain number of shareholders in such a way that only some subsets of them are able to jointly decrypt it. Several schemes and variants of secret sharing have been proposed from the seminal scheme, which are based respectively on polynomial interpolation and hyper planes intersection to the most recent approaches closely involving number theory. Secret Sharing can be beneficial in many different ways in cloud computing, which is becoming increasingly common, with rapid adoption by both industry small and medium enterprises and individual users. Among the many services provided by a cloud infrastructure, we are concerned here with cloud storage and file hosting services. Building on a highly virtualized infrastructure. These services are succeeding owing to trade and industry reasons and to the fact that the underlying infrastructure and physical location are fully transparent to the user. Preserving data confidentiality in exhaust is a key issue. The main difficulty is connected to the fact with the purpose of data is stored on a remote server which is fully easy to acquire to by the cloud overhaul provider (and can be accessible to third-party people through a malicious attack). In order to complete information

confidentiality and to triumph over this issue, it is possible to encrypt a file containing sensitive in sequence before storing it on a cloud.

Security Mechanism

Client machines are fully trusted. All of the entities (the dealer and the shareholders) run their individual protocol steps on their client equipment where keys and certificates required for encryption/ decryption and verification are stored. If a CSP (Cloud Service Provider) has to be used for share storage shareholders encrypt their Shares using a symmetric cipher before uploading them. Similarly, shareholders download shares from CSPs to their clients and decrypt them before engaging in secret restoration and cheater identification, CSPs are semi-trusted and modeled as truthful- But-inquisitive adversary. Therefore, they act according to their prescribed actions in all of the protocols they are involved in (they do not, as malicious users do try to alter stored data and communications) but it is assumed that CSPs are interested in scholarship the contents of shares Stored by shareholders and can fully access everything stored on their cloud storage infrastructure.

2. RELATED WORK

In this paper[1]" Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds" Sensitive data stored in the cloud have to be secluded from being read in the understandable by a cloud provider that is honest but-curious. Additionally, cloud-based data are increasingly being accessed by resource-constrained transportable devices for which the special consideration and communication cost must be minimized. Novel modifications to attribute-based encryption are proposed to allow sanctioned users access to cloud data based on the contentment of required attributes such that the superior computational load from cryptographic operation is assigned to the cloud provider and the total communication cost is lowered for the mobile user. In this paper [2] "Publicly Verifiable Secret Sharing" A publicly verifiable secret sharing (PVSS) scheme is a verifiable secret sharing scheme with the property that the validity of the shares distributed by the dealer can be verified by any social gathering. We present a new manufacture for PVSS schemes, which compared to previous solutions improvements both in efficiency and in the type of intractability assumptions. The running time is O(nk), where k is a security parameter, and n is the number of participants, hence essentially optimal. The intractability assumptions are the standard Diffie-Hellman assumption and its decisional variant. We present several applications of our PVSS scheme surrounded by which a new type of universally demonstrable election scheme is based on PVSS. In this paper [3]"Efficient publicly verifiable secret sharing with correctness, soundness and ZK privacy" A PVSS is a secret sharing scheme with public verification of share validity. A new all-purpose PVSS scheme is calculated to trounce the existing drawbacks. It is correct sound and efficient. Its community verification procedure is strict honest-verifier zero knowledge. In addition, it has an proficient and immediate underground recovery purpose and has no individual requirement on the secret. Another payment in this paper is that the public verification procedure has independent assessment.

3. PROBLEM DEFINITION

Sharing deals with the difficulty of securely distributing confidential information among a certain number of shareholders in such a way that only some subsets of them are able to jointly decrypt it.

- Preserving data confidentiality in clouds is a key issue.
- The main difficulty is connected to the fact that data is stored on a remote server which is fully accessible by the cloud service provider.
- Encryption makes harder unauthorized disclosure of information.

4. PROPOSED SYSTEM

Several schemes and variants of secret sharing have been proposed, from the seminal schemes which are based respectively on polynomial interpolation, and hyper planes intersection to the newest approaches closely involving number theory, such as the ones based on Remainder Theorem. Secret Sharing can be beneficial in many different ways in cloud computing, which is becoming increasingly common, with rapid adoption by both industry, small and medium enterprises, and individual users.

Benefits

- Possible to encrypt a file containing sensitive information before storing it on a cloud.
- Secret Sharing and multiple clouds.
- Providers, a scenario in which each generated share is stored on a different cloud.
- The use of multiple clouds and Secret Sharing can therefore mitigate and minimize.

5. IMPLEMENTATION

Cryptographic controls:

Encryption is the process of transforming readable information into something unreadable using an algorithm (or cipher) and a cryptographic key. The input into the process is often referred to as the plaintext and the output is known as the ciphertext. The reverse process, used to recover the plaintext is known as decryption. Broadly speaking, there are two types of encryption: symmetric (or private-key) encryption and asymmetric (or public-key) encryption.

Verification:

Verification protocols that does not even require storing public data for verification; our schemes can be used in conjunction with arbitrary secret sharing schemes, and provide cheater detection capabilities; we also introduce, in one of our schemes, a new computational problem, namely the Experiential Polynomial Root Problem (EPRP), which generalizes the Discrete Logarithm Problem Commitments can be implemented via one-way functions, as a basis for verification schemes.

Security and Privacy Protection:

The original file can still be encrypted if required, thus providing an additional security guarantee. The use of multiple clouds and Secret Sharing can therefore mitigate and minimize several risks associated to the single cloud provider scenario, such as service availability failure, data loss and/or corruption, loss of confidentiality, vender lock-in and the possibility of malicious insiders in the single cloud. Cloud computing to Shamir's secret sharing security can be enhanced, by making each of the n shareholders.

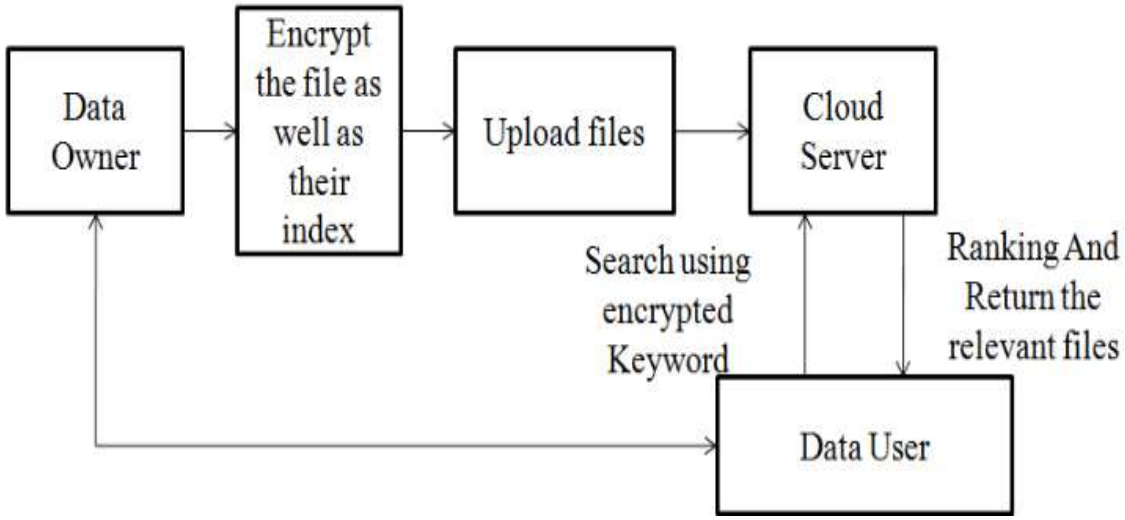

Fig.1. Secure Data Encryption

verify the others' shares, and assigning a different, private security parameter uj to each verifier; in this environment, this would mean generating n different polynomials.

CONCLUSION

Our main effort was devoted to reducing the amount of verification data for a secret sharing scheme without worsening the security properties; a new computational problem, EPRP, supposed to be harder than the DLP, has been introduced, but the derived verification schemes, missing the homomorphism property, are not extensible to additional shareholders, and the dealer must be a trusted entity, since any malicious behavior of this party cannot be detected. Further research should be carried out on the possibility of modifying the proposed problem in order to augment it with the homomorphism property, so that a resulting VSS scheme would present shareholder extensibility, and to investigate if this kind of problem can be also exploited in interactive proofs for authenticating the dealer's integrity and in public key based cryptosystems. Another possible direction for future work could regard investigating additional runtime efficiency refinements.

REFERENCES

[1] A. Shamir, "How to share a secret.," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. Blakley, "Safeguarding cryptographic keys," in Proceedings of the 1979 AFIPS National Computer Conference, (Monval, NJ, USA), pp. 313–317, AFIPS Press, 1979.

[3] M. Mignotte, "How to share a secret," in Proceedings of the 1982 Conference on Cryptography, (Berlin, Heidelberg), pp. 371–375, Springer-Verlag, 1983.

[4] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," IEEE Trans. Inf. Theor., vol. 29, pp. 208–210, Sept. 2006.

[5] P. Tysowski and M. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds," Cloud Computing, IEEE Transactions on, vol. 1, pp. 172–186, July 2013.

[6] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in Foundations of Computer Science, 1985., 26th Annual Symposium on, pp. 383–395, 1985.