REVOCABLE IDENTITY-BASED ACCESS CONTROL FOR BIG DATA WITH VERIFIABLE OUTSOURCED COMPUTING

ABSTRACT

- To be able to leverage big data to achieve enhanced strategic insight, process optimization and make informed decision, we need to be an efficient access control mechanism for ensuring end-to-end security of such information asset.
- Signcryption is one of several promising techniques to simultaneously achieve big data confidentiality and authenticity. However, signcryption suffers from the limitation of not being able to revoke users from a large-scale system efficiently.

- We put forward, in this paper, the first identity-based (ID-based) signcryption scheme with efficient revocation as well as the feature to outsource unsigncryption to enable secure big data communications between data collectors and data analytical system(s).
- Our scheme is designed to achieve end-to-end confidentiality, authentication, non-repudiation, and integrity simultaneously, while providing scalable revocation functionality such that the overhead demanded by the private key generator (PKG) in the key-update phase only increases logarithmically based on the cardiality of users.

EXISTING SYSTEM

- As data becomes “bigger”, so does users’ concerns about data security and user privacy .Leakage of sensitive user data can be extremely damaging to the individual concerned as well as the organization; thus, eroding the confidence of the users.

- On one hand, ensuring the data can only be accessible by the authorized user or system is crucial in guaranteeing confidentiality of these data.

- On the other hand, without the capability to ensure the integrity, non-repudiation and authentication of big data, decisions may be made on wrong and misleading information (e.g. data that have been altered by an attacker).

DISADVANTAGES

- Leakage of sensitive user data can be extremely damaging to the individual concerned as well as the organization.
- Decisions may be made on wrong and misleading information (e.g. data that have been altered by an attacker).

PROPOSED SYSTEM

- We propose a novel ID-based signcryption scheme with efficient revocation functionality (R-IBSC), based on the binary tree structure. In particular, our construction offers a shorter ciphertext size and faster signcryption compared with the sign-then-encrypt approach.
- Furthermore, the key-update overhead at the PKG increases logarithmically with the number of users, which is particularly attractive in a large-scale big data environment.

- Our scheme also achieves short-term key exposure resistance, and is proven to achieve indistinguishability and existential unforgeability against the chosen ciphertext attacks adaptively (shorten as IND-CCA2) and the chosen message attacks adaptively (shorten as EUF-CMA) assuming the intractability of the Decision Bilinear Diffie-Hellman (DBDH) problem and the computational Diffie Hellman (CDH) problem respectively in the well-known random oracle model

ADVANTAGES

- Data authenticity and confidentiality can be achieved using secure signature and encryption schemes, respectively.
- Signcryption, a promising security solution for big data

HARDWARE REQUIREMENTS

□ System	: PentiumIV 2.4 GHz.
□ Hard Disk	: 40 GB.
□ Floppy Drive	: 1.44 Mb.
□ Monitor	: 15 VGA Colour.
□ Mouse	: Logitech.
□ Ram	: 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : windows XP/7
- Coding Language : ASP.net,C#/java

CONCLUSION

- Motivated by the practical and operational needs to provide secure communication for big data in a cloud computing deployment, we proposed a novel ID-based signcryption scheme with efficient revocation and unsigncryption outsourcing. This is, as far as we know, the first ID-based signcryption scheme to provide both efficient revocation and unsigncryption out-sourcing. We then proved the security of the proposed scheme in the random oracle model. Extensive experimental results also demonstrated the utility of the proposed scheme.