INFO - 2196 UDK: 004.77:004.056
Primljeno/Received: 2018-11-05 Authors Review/ Pregledni rad

https://doi.org/ 10.32914/i.51.3-4.6

ACCESS CONTROL SCHEME IN CLOUD SERVICES BASED ON DIFFERENT USER ROLES

MODEL KONTROLE PRISTUPA USLUGAMA U OBLAKU NA OSNOVU RAZLIČITIH ULOGA KORISNIKA

Shanmugasundaram Singaravelan[1], Ramaiah Arun[1], Dhiraviyam Arun Shunmugam[1], Raja Veeman Vivek[2], Dhanushkodi Murugan[3]

Department of CSE, PSR Engineering College, Sivakasi, Tamilnadu, India[1]; Department of CSE, Sethu Institute of Technology, Pulloor ,Tamilnadu, India[2]; Department of CSE, Manonmaniam Sundaranar University, Tirunelveli,India[3]
Odjel za CSE, PSR Engineering College, Sivakasi, Tamilnadu, Indija[1]; Odjel za CSE, Tehnološki institut Sethu, Pulloor, Tamilnadu, Indija[2]; Odjel za CSE, Sveučilište Manonmaniam Sundaranar, Tirunelveli, Indija[3]

Abstract

The rapid development of computer technology, cloud-based services have become a hot topic. They not only provide users with convenience, but also bring many security issues, such as data sharing and privacy issue. In this paper, we present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, we divide users into private domain (PRD) and public domain (PUD) logically. In PRD, to achieve read access permission and write access permission, we adopt the Key-Aggregate Encryption (KAE) and the Improved Attribute-based Signature (IABS) respectively. In PUD, we construct new multi-authority cipher text policy attribute-based encryption (CP-ABE) scheme with efficient decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it. The analysis and simulation result show that our scheme is feasible and superior to protect users' privacy in cloud-based services.

Sažetak

Nagli razvoj računalne tehnologije, usluge temeljene na oblaku, postale su aktualna tema. Oni ne samo da korisnicima pružaju praktičnost, nego i donose mnoga sigurnosna pitanja, kao što je dijeljenje podataka i problem privatnosti. U ovom radu predstavljamo sustav kontrole pristupa s razdvajanjem povlastica na temelju zaštite privatnosti (PS-ACS). U PS-ACS shemi, podijelimo korisnike na privatnu domenu (PRD) i javnu domenu (PUD) logično. U PRD-u, da bi se postiglo dopuštenje pristupa za čitanje i dopuštenje za pisanje, usvajamo ključno šifriranje (KAE) i poboljšani potpis na temelju atributa (IABS). U PUD-u konstruiramo novu shemu šifriranja (CP-ABE) koja se temelji na pravilima šifriranog teksta s učinkovitim dešifriranjem kako bismo izbjegli probleme s jednom točkom neuspjeha i kompliciranе distribucije ključeva i dizajnirali učinkovitu metodu opoziva atributa za nju. Rezultati analize i simulacije pokazuju da je naša shema izvediva i superiorna za zaštitu privatnosti korisnika u uslugama temeljenim na oblaku.

I. INTRODUCTION

The rapid development of cloud computing, big data and public cloud services have been widely used. Users can store their data in the cloud service and rely on the cloud service provider to give data access to other users. However, the cloud service provider can no longer be fully trusted. Because it may give data access to some illegal users or attackers for profit gain. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. Since traditional access control strategy /**1**/ cannot effectively solve the security problems that exist in data sharing, various schemes to achieve encryption and decryption of data sharing have been proposed. In 2007, Bettencourt et al. /**2**/ first proposed the cipher text policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. Attrapadung et al. /**3**/, /**4**/ came up with two us-er-revocable ABE scheme. However, they are not applicable in the outsourcing environment. In 2011, Hur et al. /**5**/ put forward a fine-grained revocation scheme, but it can easily cause key escrow issue. Lewko et al. /**6**/ used multi-authority ABE (MA-ABE) to solve key escrow issue. But the access policy is not flexible. Later, Li et al. /**7**/ presented a data sharing scheme based on systemic attribute encryption, which endows different access permissions to different users. However, it lacks of efficiency. Xieet al. /**8**/ presented a revocable CP-ABE scheme. Compared with Hur's scheme, in the key update phase, the computation load of the data service manager will be reduced by half. Liang et al. /**9**/ proposed a CP-ABE proxy encryption scheme which supports any monotonic access structures. However, their construction which is built in the Composite order bilinear group. cannot be converted to the prime order bilinear group. In 2014, Chu et al. /**10**/ proposed Key-Aggregate Encryption algorithm, which effectively shortens the length of the cipher text and the key, but only for the situation where the data owner knows user's identity. The above schemes only focus on one aspect of the research, and do not have a strict uniform standard either. In this paper, we present a more systematic, flexible and ef-ficient access control scheme. To this end, we make the following main contributions: We propose a novel access control sys-tem called PS-ACS, which is privilege sepa-ration based on privacy protection. To achieve read access permission, in PRD, the Key-Ag-gregate Encryption (KAE) scheme which greatly improves access efficiency is adopted. And in PUD, we construct a new multiauthority cipher text policy attribute-based encryption (CP-ABE) scheme with efficient decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it. Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) /**11**/, /**12**/, /**13**/ scheme to enforce write access control in PRD. In this way, the user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file.We provide security and performance analysis of our proposed PS-ACS scheme. The functionality and simulation results provide data security in acceptable performance impact, and prove the feasibility of the scheme. The remaining of this paper is organized as follows. We first provide some preliminaries in Section 2. In Section 3, we give the definition of the system model. Then, we present the access control scheme in PRD in Section 4 and the access control scheme in PUD in Section 5. Section 6 gives the security and the performance analysis of our scheme. Finally, the conclusion is given in Section 7.

2. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

Our existing system enhances a general approach to protect the data is encryption

methodology, they are keyword based encryption system and it supports for plain text data. Fully homomorphic encryption is used to solve the problem of the data user. Searchable encryption schemes are very efficient, its functionality and security is well and also allows users to search in the cipher text in cloud storage.

2.2 DISADVANTAGES

The single keyword search is not smart enough to support advanced queries and it is unrealistic since it causes high communication cost.

The time complexity of search in the number of keywords in dictionary and the time complexity of trapdoor construction is also very high. Due to the size of indexes, the space consumption also becomes larger.

3. PROPOSED SYSTEM

We proposed an access control system, which is privilege separation based on privacy protection. A number of hierarchical authorisation structures are also presented, which can be used in organizations or companies to meet the requirement of authorization grant right decentralization. The domain authorities will distribute the security parameters to users or subdomain authorities.

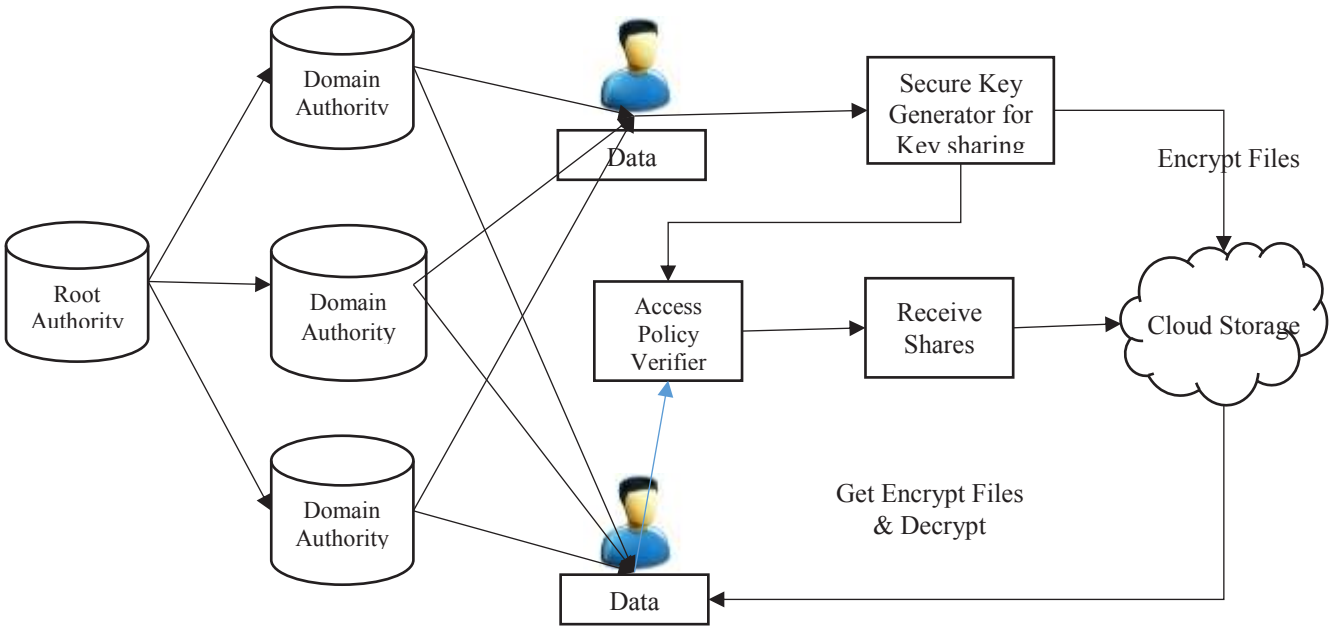

Fig.1 System architecture

In Fig.3.1 describe the architecture efficient construction for those schemes, denoted as Secret Shares Algorithm in Encryption Based Construction, which assigns to each class a single private information, whereas, the public information depends on the number of classes, as well as on the number of edges in the hierarchy. The security of the proposed construction relies on the ones of the underlying encryption and secret sharing schemes using Shamir Secret Sharing Algorithm.

3.1 ADVANTAGES

The proposed method achieves high efficiency of privacy protection. We present a secure authentication protocol for the hierarchical authorization structure in the cloud big data access control system to authenticate authorities or users. We extend the protocol to support multiple levels authentication in the hierarchical attribute authorization structure. Our methodology provides security properties of forgery attack resistance, replay attack resistance and privacy preservation.

4. MODULES DESCRIPTION

4.1 Root Authority

The root authority is the top authority and responsible for generating system parameters.

Fig 4.1 describes the root authority will first login to the system and verify whether it is a valid domain authority. Authorise top-level domain authorities (DA) by creating Master Key.

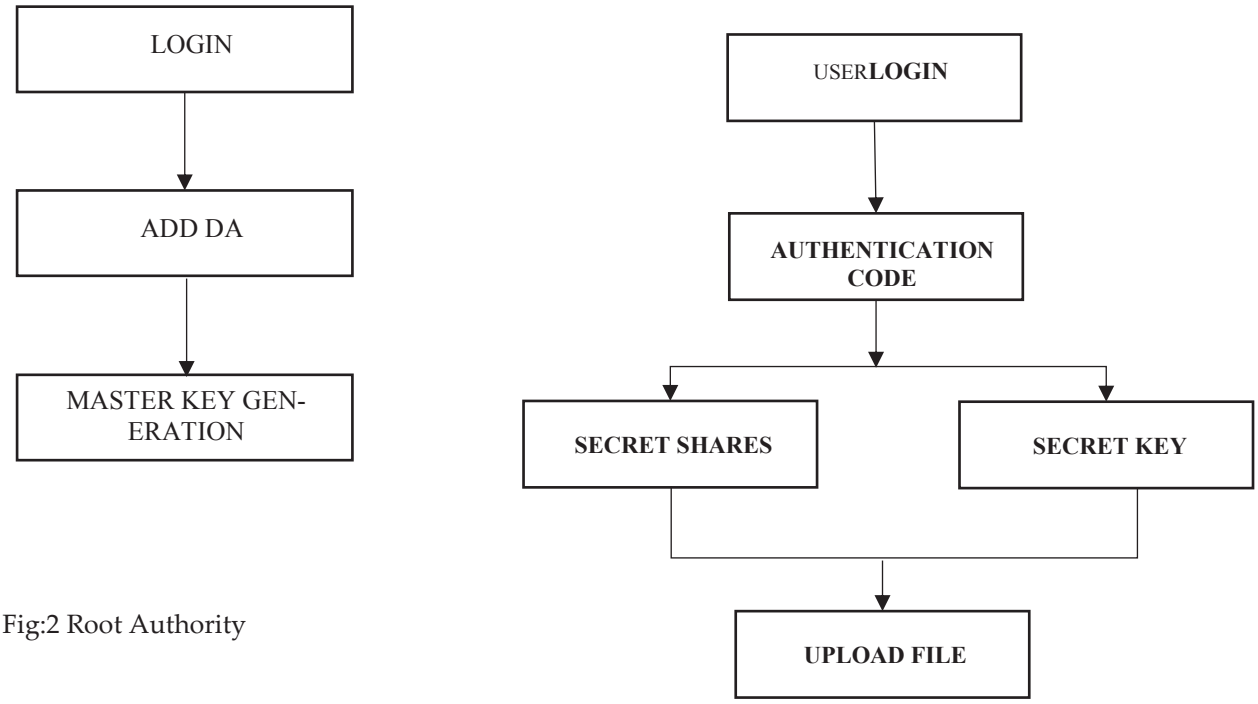

Fig:2 Root Authority

4.2 Domain Authority

Domain Authority (DA) is managed by its parent domain authority or a trusted root authority. Fig 4.2 describe the inherited structure of domain authority reduces the computation and disperses the burden and risk of the authority of the central attribute authority. After obtaining the master key from root authority, DA will login to the system after master key verification and authorize the next level domain authorities or users in its domain. Enrols the next level data owner and user by generating Unique Authentication Code. DA can view the user data access request in its domain and grant access permission after verifying access policy of the corresponding user.

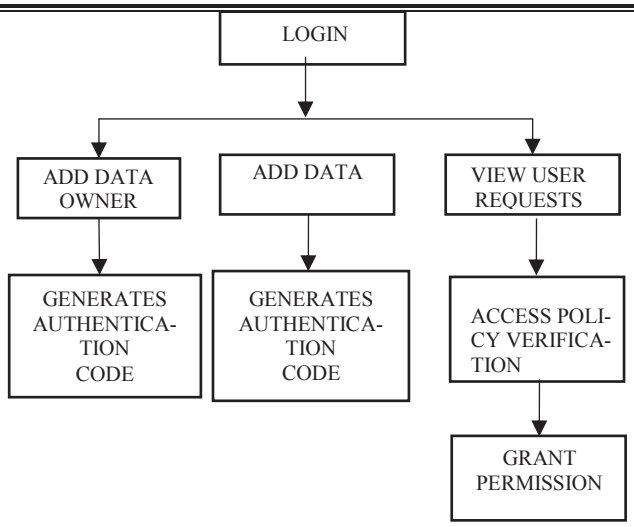

Fig 3.Domain Authority

4.3 Data Owner

The Data Owner login to the system after verifying unique authentication code. The Fig 4.3 describe DOwill encrypt the file using secret key and outsource the data file into the cloud. To ensure the confidentiality and integrity of the data, DOadditionally DO generates certain pieces of Secret shares for each data file stored in the cloud.

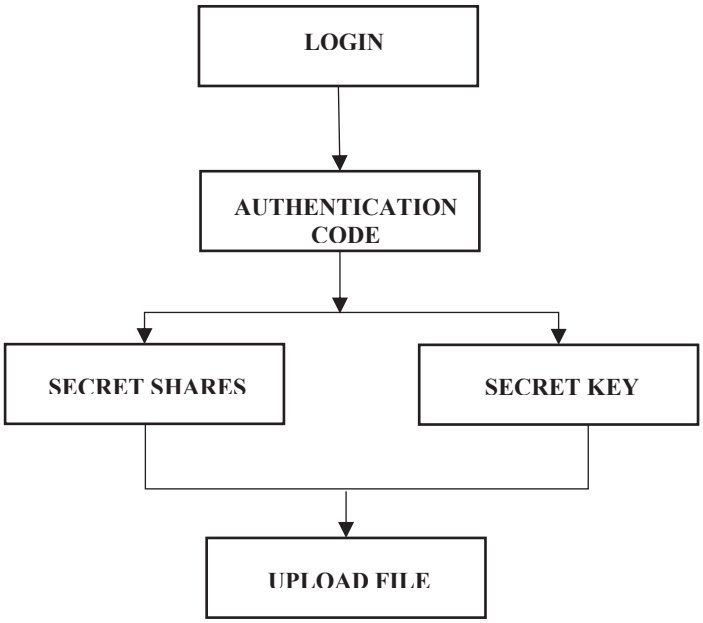

Fig:4. Data Owner

4.4 Data User

The Data User (DU) login to the system after verifying unique authentication code. Fig 4.4 describe the DU can view the data files outsourced in the cloud. DU send data access request to the corresponding domain authority. DU will be provided secret shares by the domain authority after Access Policy verification. DU should submit the Secret shares corresponding domain authority.

After verification only DU can get Secret Key to download the decrypted data file.

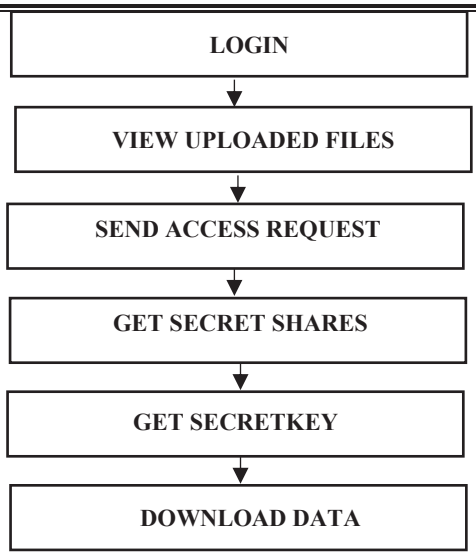

Fig. 5 Data User data downloading

5. CONCLUSION

Secure sharing of data plays an important role in cloud computing, it can realize data confidentiality in the untrusted environment of server-end, fine-grained access control and large-scale dynamic authorization which are the difficult problems to solve the traditional access control. This paper proposes a structure of hierarchical authority based on cloud computing which reduces the burden and disperses the risk of the single authority. In addition, we have implemented Shamir Secret Sharing Algorithm for high level security, this shows our scheme has good adaptability and scalability in cloud computing.

6. FUTURE ENHANCEMENT

Our scheme has lower computational and communication overhead, which has a promising future in secure authentication in cloud big data. In further research, we intend to focus on making the Secret Sharing algorithm simpler and more efficient along with making it even more suitable for access control in a cloud environment.

Notes

/1/ Yu Sh, Wang C, Ren K. (2019). "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", *Proceedings of IEEE Conference on Information Communications 2010*,pp 1-9.

/2/ Bethencourt J, Sahai A, Waters B. (2007)., "Ciphertext-Policy Attribute-based Encryption", *IEEESymposium on Security and Privacy*, vol. 2008,no. 4, pp. 321-334.

/3/ Attrapadung N, Imai H. (2009). "Conjunctive Broad-cast and Attribute-Based Encryption", *Proceed-ings of Pairing-based Cryptography - Pairing 2009*, vol. 5671, pp. 248-265.

/4/ Attrapadung N, Imai H. (2009). "Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes", *Proceedings of Cryptography and Cod-ing 2009*, pp. 278-300.

/5/ Hur J, Noh D K. (2011). "Attribute-based Access Control with Efficient Revocation in Data Outsourc-ing Systems", *IEEE Transactions on Parallel andDistributed Systems*, vol. 22, n o. 7, pp. 1214-1221.

/6/ Lewko A, Waters B. (2011). "Decentralizing Attribute-based Encryption", *Proceedings of Ad-vances in Cryptology-EUROCRYPT 2011 - 30thAnnual International Conference on the Theory and Applications of Cryptographic Techniques*,pp 568-588.

/7/ Li M, Yu Sh, Zheng Y. (2013). "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-based Encryption", *IEEE Transactions on Parallel and Distributed System*, vol. 24, no. 1, pp. 131-143.

/8/ Xie X, Ma H, Li J, et al. (2013). "New Ciphertext-Policy Attribute-based Access Control with Efficient Revocation", *Proceedings of* Information and Communication Technology 2013, pp. 373-382.

/9/ Liang K, Man H A, Susilo W, et al. (2014). "An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data

Sharing", *Information Security Practice andExperience*, pp. 448-461.

/10/ Chu C K, Chow S S M, Tzeng W G. (2014). "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", *IEEE Transactions on Paralleland Distributed Systems*, vol. 25, no. 2, pp. 468-477.

/11/ Li J, Kim K, (2010). "Hidden Attribute-based Signatures without Anonymity Revocation", *InformationSciences*, vol. 180, no. 9, pp. 1681-1689.

/12/ Maji H K, Prabhakaran M, Rosulek M. (2011). "Attribute-based Signatures", *Proceedings of RSAConference 2011*, pp. 376-392.

/13/ Kumar S, Agrawal S, Balaraman S, et al. (2010). "Attribute based Signatures for Bounded Multi-level Threshold Circuits", *Proceedings ofPublic Key Infrastructures, Services and Applications-European Workshop, Europki 2010*, pp.141-154.