International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Forward Security & Cipher text policy on Data Privacy preservation by shared authority encryption

Mr.V.Sudarshan[1]

[1]Associative Professor ,Department of Computer Science & Engineering,Khammam Institute of Technology & Sciences(KITS),Khammam,T.S-India, sudharshan.cse@gmail.com.

Mr.A.Dileep Kumar [2]

[2] Asstistant Professor ,Department of Computer Science & Engineering, Khammam Institute of Technology & Sciences(KITS),Khammam,A.P-India, achinni.dileepkumar@gmail.com

Ms.Shaik Farzana[3]

[3] PG Scholars

Science & Engineering,Khammam Institute of Technology & Sciences(KITS),Khammam,T.S-India

Abstract

Cloud computing is emerging as a prevalent data interactive paradigm to realize user's data remotely stored in an online cloud server.. A cloud storage system, consisting of an accumulation of storage servers, provides long-term storage accommodations over the Internet. Storing data in a third party's cloud system causes solemn concern over data confidentiality. Constructing a secure storage system that fortifies multiple functions is challenging when the storage system is distributed and has no central ascendancy. We propose a proxy re-encryption scheme that fortifies encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. Our method plenarily integrates encrypting, encoding, and forwarding. We analyze and suggest congruous parameters for the number of replicas of a message dispatched to storage servers and the number of storage servers queried by a key server.

Keywords: Cloud computing, authentication protocol, privacy preservation, shared authority, encryption,Cipher text policy, Data anonymity, Forward Security

.

1. Introduction

CLOUD computing is a promising information technology architecture for both enterprises and individuals. It launches an alluring data storage and interactive paradigm with conspicuous advantages, including on-demand self-accommodations, ubiquitous network access, and location independent resource pooling. Towards the cloud computing, typical accommodation architecture is anything as an accommodation (XaaS), in which infrastructures, platform, software, and others are applied for ubiquitous interconnections. Recent studies have been worked to promote the cloud computing evolve towards the cyber world of accommodations.

Subsequently, security and privacy issues are becoming key concerns with the incrementing popularity of cloud accommodations. Conventional security approaches mainly fixate on the vigorous authentication to realize that a utilizer can remotely access its own data in on-demand mode. Along with the diversity of the application requisites, users may want to access and apportion each other's sanctioned data fields to achieve pro- ductive benefits, which bring incipient security and privacy challenges for the cloud storage. In the cloud storage predicated supply chain management; there are sundry interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users which are sanctioned to access the sanctioned data fields, and different users own relatively independent access ascendant entities. It signifies that any two users from diverse groups should access different data fields of the same file. There into, a supplier intentionally may want to access a carrier's data fields, but it is not sure whether the carrier will sanction its access request. If the carrier relicts its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Authentically, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly kens that its request will be reelected by the carrier. It is adamant to exhaustively disclose the supplier's private information without any privacy considerations.

Case 1: The carrier withal wants to access the supplier's data fields, and the cloud server should appraise each other and transmit the shared access ascendancy to the both users.

Case 2: The carrier has no interest on other users' data fields; consequently its sanctioned data fields should be felicitously bulwarked, mean while the supplier's access request will additionally be concealed.

Case 3: The carrier may want to access the retailer's data fields, but it is not certain whether the retailer will accept its request or not. The retailer's sanctioned data fields should not be public if the retailer has no fascinates in the carrier's data fields, and the carrier's request is withal privately obnubilated. Towards above three cases, security bulwark and privacy preservation are both considered without revealing sensitive access desire cognate information

In the cloud environments, a reasonable security protocol should achieve the followingrequirements.

Authentication: a legal user can access its own data fields, only the authorized partial or entire datafields can be identified by the legal user, and any forged or tampered data fields cannot deceive thelegal user.

Data anonymity: any irrelevant entity cannot recognize the exchanged data and communication stateeven it intercepts the exchanged messages via an open channel.

User privacy: any irrelevant entity cannot know or guess a user's ac-cess desire, which represents auser's interest in another user's authorized data fields. If and only if the both users have mutualinterests in each other's authorized data fields, the cloud server will inform the two users to realizethe access permission sharing.

Forward security: any adversary cannot correlate two communication sessions to derive the

priorinterrogations according to the currently captured messages.

In this paper, we address the aforementioned privacy issue to propose a proxy based privacy preservingauthentication protocol for the cloud data storage, which realizes authentication andauthorization without compromising a user's private information. The main contributions are asfollows.

- Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.
- Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.
- Apply cipher text policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

2. Related Work

2.1 Existing System:

Despite the tremendous benefits, outsourcing computation to the commercial public cloud is withal depriving customers' direct control over the systems that consume and engender their data during the computation, which ineluctably brings in incipient security concerns and challenges towards this promising computing model.

On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information sets. The unauthorized information leakage, sensitive data have to be encrypted afore outsourcing. So as to provide end to- end data confidentiality assurance in the cloud and beyond. unauthorized information leakage, sensitive data have to be encrypted afore outsourcing. So as to provide end to- end data confidentiality assurance in the cloud and beyond. For example, for the computations that require a substantial amount of computing resources, there are sizably voluminous financial incentives for the cloud to be "lazy" if the customers cannot tell the correctness of the output. Besides, possible software bugs, hardware failures, or even outsider attacks might additionally affect the quality of the computed results.

Disadvantage of Existing System:

- The cloud is intrinsically not secure from the viewpoint of customers without providing a mechanism for secure computation outsourcing so to protect the sensitive input and output information of the workloads.
- The various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi hones model.

2.2 Proposed System:

A shared ascendancy predicated privacy-preserving authentication protocol (SAPA) to address above

privacy issue for cloud storage. In the SAPA, shared access ascendancy is achieved by in nominate access request matching mechanism with -*security and privacy considerations (e.g., authentication, data anonymity, utilize privacy, and forward security attribute predicated access control is adopted to realize that the utilizer can only access its own data fields proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, macrocosmic compos faculty (UC) model is established to prove that the SAPA theoretically has the design correctness.

It betokens that the proposed protocol realizing privacy-preserving data access ascendancy sharing is captivating for multi-utilizer collaborative cloud applications. The outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. Planarity homomorphism encryption (FHE) scheme, a general result of secure computation outsourcing has been shown viable in theory, where the computation is represented by an encrypted combinational Boolean circuit that sanctions to be evaluated with encrypted private inputs.

Advantages of Proposed System:

The outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information can be secured utilizing private computing.

3. Implementation

The Implementation of the System is follows

- **Distributor**
- **Supplier**
- **Carrier**
- **Customer**
- **Authentication**
- **Registration**

Registration:

The system has a process of registration. Every user need to submit their complete details including user name and password in the form of registration. Whenever a user registration completed then only a user can get log in into the system by using his user id and password.

Login:

In this module user can give the user id and password after giving that we are checking that valid person or not means here we are giving security for our application.

The login page will restrict the UN authorized users. A user must provide his credential like user Id and password for log into the system. For that the system maintains data for all users. Whenever a user enters his user id and password, it checks in the database for user existence. If the user is exists he can be treated as a valid user. Otherwise the request will throw back.

Distributor:

Customer wants to order products from a distributor with the requirement that these must be delivered before the drop-dead date. To satisfy such a request, the distributor will try to find a supplier that has the products available. If found, he will search for a carrier that is able to deliver the products before the drop-dead date. If both the supplier and the carrier are able to fulfill the demands of the customer, the

distributor will report to the customer that he can fulfill the order.

Supplier:

Supplier can manage products in the system. He can view all types of products details. He taken request from the distributor. If the request result from the supplier is positive, the BPEL process seeks a suitable carrier to deliver the products. Otherwise, the process will return a fault message indicating no suitable supplier is available for the supply. He can manage the personal details.

Carrier:

He took request from the distributor. if a carrier is found, the process will ask the supplier to dispatch the products, and ask the carrier to deliver the products. Otherwise, the process will return a fault message indicating no suitable carrier is available for the delivery. After the successful delivery of the products to the customer, the process is informed by the distributor with the positive result, and it returns a success message. He can manage the personal details.

Customer:

He is a registered user to the Site. This user can view all products and product details. He send the request for products to the distributor and receive the suitable response from distributor. He can manage the personal details.

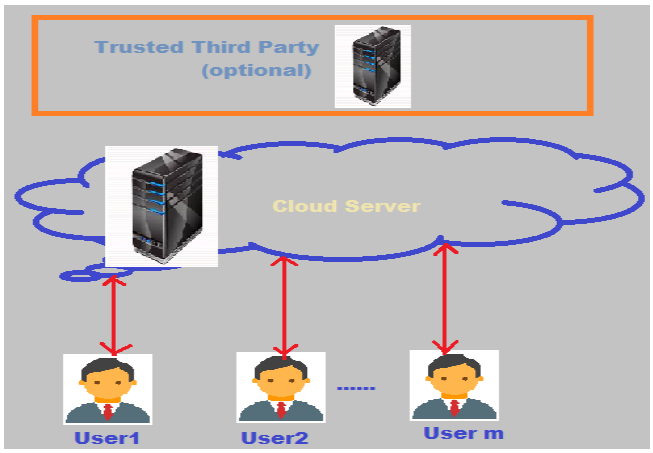

Fig.1 illustrates a system model for the cloud storage architecture, which includes three mainnetwork entities: users (Ux), a cloud server (S), and a trusted third party

User: an individual or group entity, which owns its data stored in the cloud for online datastorage and computing. Different users may be affiliated with a common organization, and areassigned with independent authorities on the certain data field.

Cloud server: an entity, which is managed by a particular cloud service provider or cloudapplication operator to provide data storage and computing services. The cloud server is regarded asan entity with unrestricted storage and computational resources.

Trusted third party: an optional and neutral entity, which has advanced capabilities on behalfof the users, to perform data public auditing and dispute arbitration.

In the cloud storage, a user remotely stores its data via online infrastructures, platforms, orsoftware for cloud services, which are operated in the distributed, parallel, and cooperative modes.During cloud data accessing, the user autonomously interacts with the cloud server without externalinterferences, and is

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

assigned with the full and independent authority on its own data fields. It isnecessary to guarantee that the users' outsourced data cannot be unauthorized accessed by otherusers, and is of critical importance to ensure the private information during the users' data accesschallenges.

In some scenarios, there are multiple users in a system (e.g., supply chain management), and theusers could have different affiliation attributes from different interest groups. In the system model,assume that point-to-point com-munication channels between users and a cloud server are reliablewith the protection of secure shell protocol (SSH). The related authentication handshakes are nothighlighted in the following protocol presentation.

Experimental Work

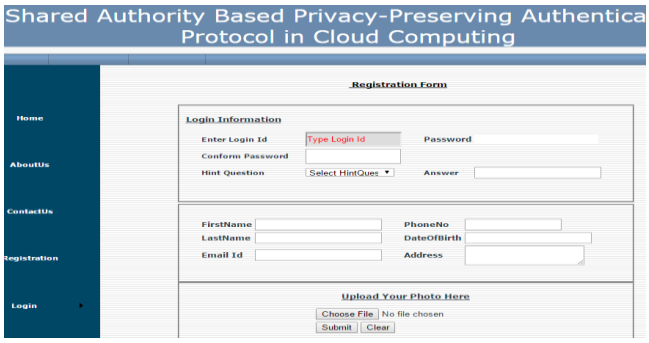

Fig 2: Registration form of the System.

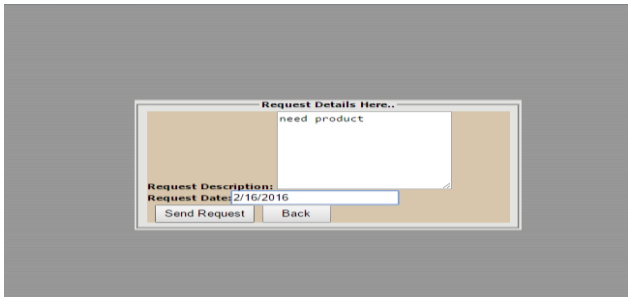

Fig 2: Customer Request details Page.

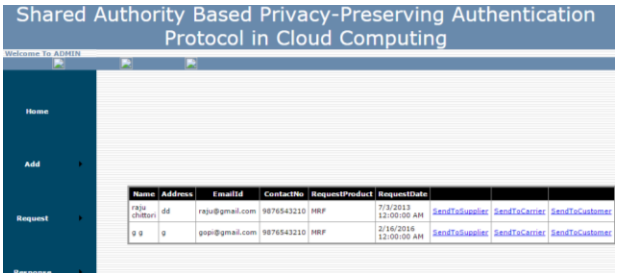

Fig 3: Customer Request Processing Page.

4. Conclusion

In this work, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for privacy preservation in cloud applications.

5. References

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards andTechnology, USA, 2009.

[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Net-working and Communication Challenges," IEEECommunications Magazine, vol. 50, no. 9, pp, 24-25, 2012.

[3] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Key Challenges in Cloud Computing to Enable theFuture Internet of Services," IEEE Internet Computing, [online]

ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493,2012.

[4] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE InternetComputing, vol. 14, no. 5, pp. 14-22, 2010.

[5] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architec-ture for Cloud Computing," Computer, vol. 45, no.7, pp. 73-78, 2012.

[6] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloudStorage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

[7] H. Wang, "Proxy Provable Data Possession in Public Cloud-s," IEEE Transactions on Services Computing, [online]ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.

[8] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in CloudComputing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2012.

[9] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in theCloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615,2012.

[10] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Pol-icy Based Content Sharing in Public Clouds," IEEETrans-actions on Knowledge and Data Engineering, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891,2012.

[11] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEETransactions on Informa-tion Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

V.Sudharshan received the M.Tech degrees in computer science Engineering and Information Technology from the JNTUH University, Hyderabad, in 2005 and 2010, respectively, and is currently pursuing the Ph.D. degree in Computer Science & Engineering at the JNTUH—Hyd..He has a vast experience in network-related software-development from several startup companies. His research interests include Secure Cloud Computing, content caching, cellular networks, and traffic redundancy elimination.

Dileep Kumar received the M.Tech degree in Computer Science & Engineering from the University JNTUH, Hyderabad.