

Institutional Sign In

BrowseMy SettingsGet HelpSubscribe

Advertisement

Full Text

Abstract

Authors

Figures

References

View All

Citations

View All Authors
Keywords

Back to Top

Browse Conferences > Global Trends in Signal Proce...

Group data searching and sharing using key aggregate cryptosystem

Sign In or Purchase
to View Full Text

13
Full
Text Views

2
Author(s)

S. K. Sonkar ; S. P. Wakchaure

Abstract	Authors	Figures	References	Citations	Keywords	Metrics	Media
----------	---------	---------	------------	-----------	----------	---------	-------

Abstract:

Sharing encrypted data with different users gained great attention in the cloud environment. There have some security issues like data leaks during data sharing, key management of shared data etc. In our project we developed a system which enables secure data sharing in the group of users as well as efficient key management. In our proposed system we used public key cryptography for securely storing and sharing data in cloud. We have created secure constant cipher text which is impartial of data size. It is possible to share data and to give authorized rights for decryption of any set of cipher text. Along with the encrypted data a searchable index is generated to provide search over the encrypted data. The data owner can share subset of files with other users by authorizing them an access rights and constant size of aggregate key. By doing this we are confidential about other outside files as those files cannot be decrypted using the given key. As per access rights search can be applied over restricted data set. Search can also be applied for synonym words. System performance and efficient index generation are the key aspect of our project. Experimental results show that security & efficiency is greatly improved with our proposed scheme.

Published in: Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), 2016 International Conference on

Date of Conference: 22-24 Dec. 2016

Date Added to IEEE Xplore: 26 June 2017

ISBN Information:

INSPEC Accession Number: 16980459

DOI: 10.1109/ICGTSPICC.2016.7955291

Publisher: IEEE

Conference Location: Jalgaon, India

Advertisement

Download PDF

Download Citations

View References

Email

Print

I. Introduction

CLOUD storage development is the most encouraging solution for providing pervasive, user-friendly and instant access for the huge data shared over an internet. Sharing personal data, photos, post, texts etc is now popular trend in social networking application based on cloud storage. Many business firms, institutes addicted to outsource their data to the cloud for its management. With data outsourcing approach user also have worry about an unintended leaks of data in cloud. In this paper we proposed "KASE"(Key Aggregate Searchable Encryption) approach for secure data sharing and efficient key management. Our system provides the better solution for previously noticed problems such as, Public Key Encryption (PKE) with keyword search approach. In this approach users have their own data and they wish to upload the data to a third-party database in which they may not trust [7]. This approach is complex due to computational Diffie-



- Request Permissions
- Export to Collabratec
- Alerts

Hellman problem.

Read document

Keywords

IEEE Keywords

Cloud computing, Encryption, Aggregates, Ciphers, Keyword search

INSPEC: Controlled Indexing

authorisation, public key cryptography

INSPEC: Non-Controlled Indexing

group data searching, group data sharing, key aggregate cryptosystem, encrypted data sharing, cloud environment, security issues, data leaks, key management, secure data sharing, public key cryptography, data storing, secure constant cipher text, data size, authorized rights, decryption, searchable index, data owner, authorization, access rights search

Author Keywords

Cloud Storage, Data Sharing, Privacy, Searchable encryption, decryption

Authors

S. K. Sonkar
Department of Computer Engineering, AVCOE, Sangamner, SP Pune
University, India

S. P. Wakchaure
Department of Computer Engineering, AVCOE Sangamner, SP Pune
University, India

Related Articles

Inter-domain security for Mobile IPv6
M. Laurent-Maknavicius; F. Dupont

An effective approach for authentication of mobile users
N. El-Fishway; M. Nofal; A. Tadros

Healthcare information systems using digital signature and synchronized smart cards via the Internet
Won Jay Song; Byung Ha Ahn; Won Hee Kim

Application decomposition for high-speed network processing platforms
N.A. Nikolaou; J.-A. Sanchez P; T. Orphanoudakis; D. Pollatos; N. Zervos

A quality-based cost distribution charging scheme for QoS multicast networks
A. Bueno; R. Fabregat; P. Vila

Format-compliant selective scrambling for multimedia access control
Wenjun Zeng; Jiangtao Wen; M. Severa

Spare parts expense management system [semiconductor manufacturing]
D. Yao; C. Blouin; M. Cavanaugh; G. Boldman; B. Alvarez; S. Miraglia; L. Hungerford

Sequential imaging and analysis of erythrocyte aggregation

Full Text

Abstract

Authors

Figures

References

Citations

Keywords

Back to Top

S. Jayavanth; M. Singh; K. Jagadeesan

Design of a microfabricated cell straining device for investigating cellular response to finite mechanical strains

J.C. Selby; M.A. Shannon; S.A. Boppart

Charging and accounting system design for the multi-service Internet
Hakju Kim

Full Text

Abstract

Authors

Figures

References

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

- » Communications Preferences
- » Profession and Education
- » Technical Interests

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » Contact & Support

Citations
Keywords

Back to Top

About IEEE *Xplore* | Contact Us | Help | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.