International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 18 (2015) pp 38851-38854
© Research India Publications. http://www.ripublication.com

Security of Shared Data through Efficient Data Revocation in Financial Market

Krishna Kumar Singh,
Assistant Professor, Amity University, Sec-125, Noida, U.P. kksingh1@amity.edu

Dr. Priti Dimri,
Associate Professor and Head, Dept. of Computer Science, GBPEC, Pauri, Uttarakhand. pdimri1@gmail.com

Himanshu Pathak,
Assistant Professor, Dept. of Computer Science, GIMT, Gr. Noida him.786@gmail.com

Abstract

Financial market security in the era of big data is the major challenge. Data requires for the financial forecasting is not been shared due to privacy and security concerns of the data owners. Owners of the valuable data are hesitating to share data in the public domain. Even most advanced tools of information technologies are fail disseminate desire information to the customer because of scarcity of desire data. Lack of faith among data owners on share data based technologies is becoming main hindrance. Decision making in the financial market is continuous process and it is based upon various socio – economic – political factors. Cost effective green technologies like cloud and big data is efficient enough to deal with data analytics for financial forecasting. To deal with the share data security in efficient market hypothesis based financial market needs new customized information security model to ensure various security concerns of the data owners. User-friendly information technology in the secure environment will create long term faith in the financial market. This paper deals with the security issues of share data in the era of green computing and provide customized model by data revocation.

Key words: financial market, Green computing, efficient market hypothesis, financial data security, decision making, financial forecasting, data revocation.

Introduction:

Data sharing is barren truth of the day and industries will not survive without dealing with the shared data. We are living in the era of global village and so all are connected in every respect. Financial market is not an exception. Analytics of the shared data available in unstructured manner is the big challenge for us. We are banking on the various technologies developed for the shared data but availability of relevant data is one of the major concerns for the data scientists. Data owners are still hesitating to share their data in the public domain due to various concerns of ownership and security of data. In this environment, dissemination of desired information to the public is tough. Financial market forecasting is an area where we need various data from socio – economic – political situation of the globe. Availability of data in the third world countries is very less and it creates unfaithfulness in the investment scenario in the market. Majority of people is not taking part the stock markets and markets are run by few peoples. Mass participation in the stock markets will be only ensure by taking more preventive majors in the stock market and create long term faith. Indian market has its own socio – economic challenges like low education rate, poverty, malnutrition etc. Human Index parameters are very low. Traditionally, active intermediaries in the market are working under a close environment where sharing of data for the decision making is less. Indian national exchanges like NSE (National Stock Exchange) and BSE (Bombay Stock Exchange) is shifting towards cloud computing. Efficient market hypothesis advocates reaction of market on each information. For the stable and efficient market, it’s quite compulsory that data must be integrated at the large extent and to be shared among every stack holders. Cloud computing data inculcates many challenges also like ownership, security, authenticity of data. Security of share data in the financial market is the major concern and need to address properly. Cloud computing is providing many benefits like SaaS, IaaS, Pay as you go etc but cloud computing used in the stock market decision making process is different from other computational areas. Financial marking forecasting needs various interrelated data and it doesn’t meant for only prices of the stock but it is an integrative approach of stock prices, socio – economic - political factors. Dissemination of information to the public is only being ensured by sharing of connected data and applying technologies to analyze the same. Multi read and multi write environment of shared data based technologies will be fit for the market analyst but security concerns of the shared data environment among data owners are the big hindrance. Security concerns of the data are stopping relevant data to be shared among people. And finally it stops common people to participate in the market which ultimately leads to the chaotic market conditions. To create stability in the financial market, we must ensure larger participation of the people in the financial market. To stop chances for misbehavior of financial market, this paper deals with the security issues of the share data in the financial market by ensuring data revocation.

Literature Review:

There is dearth of literature available on the information security issues of financial market in the era of green technologies. Till now IT security measures used in the market are conventional and based on traditional values and ethos. Emergence of Big Data and related technologies are shifting towards new arena. River information model for integration of scattered financial information is one of the efficient ways to deal with shared data of financial market and its refinement in cloud computing and other green technologies [6 - 9]. Security measures of financial information need more customization to meet current demands in the era of efficient computing. The privacy of personal data in RFID systems by extending the framework of Online Personal Data Licensing (OPDL) and applying the framework to RFID environment was introduced then after. Licensing issues may occur while collecting data via RFID technologies. Personal data will only collect after valid license and permission from the concern authority. Individuals can control who have licenses and the content of the licenses easily [13]. Privacy and security is a key issue for financial data in cloud based data storage technologies. Efficient framework for cloud storage is design which includes an interactive protocol and an extirpation-based key derivation algorithm, which are combined with lazy revocation, multi-tree structure and symmetric encryption to form a privacy-preserving [11]. Online social networks (OSNs) are attractive applications which enable a group of users to share data and stay connected. Facebook, Myspace, and Twitter are among the most popular applications of OSNs where personal information is shared among group contacts. Due to the private nature of the shared information, data privacy is an indispensable security requirement in OSN applications. For the security of OSNs a new privacy-preserving scheme for data sharing in OSNs is implemented, with efficient revocation for deterring a contact's access right to the private data once the contact is removed from the social group. In addition, this scheme offers advanced features such as efficient search over encrypted data files and dynamic changes to group membership [4]. Still, authenticity and integrity of messages are primary requirements in a tactical operation of mobile network, so identity management must be offered in some form. This requires that the identity management operating in the tactical zone is able to authenticate principals and control access privileges across security domains. For the sole purpose of authentication (and subsequent access control), authentication protocols are often over engineered since they also provide privacy protection, DOS protection and even non-repudiation. A cross domain identity management protocol which relies on less connectivity is already introduce, it sends fewer messages and maintains a weaker binding between domain authorities. Identity statements do not offer a revocation mechanism and circumvent the familiar certificate validation problem [1]. Revocation in cloud based distributed computing is the core issues of security in the contemporary era. Literature is full of security issues but few are available on cloud security issues for financial market data. For the mobile social network, an efficient and secure data revocation scheme was address to inside attacks based on an attribute-based encryption technique. As a result, proper data behavior is encouraged, inside attacks are reduced, and network security is enhanced [14]. In 2010, By using online Personal Health Record (PHR) as a case study, search capability authorization has introduce that reduces the privacy exposure resulting from the search results, and establish a scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data. Two novel solutions for APKS based on a recent cryptographic primitive, Hierarchical Predicate Encryption (HPE) exist but APKS enable efficient multi-dimensional keyword searches with range query, allow delegation and revocation of search capabilities [10]. In order to meet the authentication requirement of the revoking frequently and dynamic network environment, a new revocation scheme for the cloud computing environment is proposed that's include entering, leaving, revoking and authentication of entities are implemented based on the public key cryptography [15]. A new CP-ABE scheme that the data owners can fully control their outsourced shared data. It also resolves the issue of revocation including the entire data access privilege and just partial access right of the data, i.e., a subset of his/her attributes [16]. The rewriting query algorithm using a privacy-aware model like PrivOrBAC is being also used [12]. We can now outsource data backups off-site to third-party cloud storage services so as to reduce data management costs. However, we must provide security guarantees for the outsourced data, which is now maintained by third parties. A new design and implement FADE, a secure overlay cloud storage system that achieves fine-grained, policy-based access control and file assured deletion. It associates outsourced files with file access policies, and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. To achieve such security goals, FADE is built upon a set of cryptographic key operations that are self-maintained by a quorum of key managers that are independent of third-party clouds [17]. In a paper by Prof. Jin Li and his team, aimed at tackling the critical issue of identity revocation, he introduced outsourcing computation into IBE for the first time and proposes a revocable IBE scheme in the server-aided setting. His scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and data to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique [3]. Proxy re-signature is the one of the methods for revocation and implements security. In addition to it, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, this mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud [2]. An expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, revocable multi-authority CP-ABE scheme was introduce and apply it as the underlying techniques to design the data access control scheme. Attribute revocation method can efficiently achieve both forward security and backward security [5]. All this development contributes to the security of the cloud computing based financial data but financial market in the third world countries are facing different problems. Data revocation method will be one of the best methods to secure data in the shared environment.

Problem Statement:

Information security is the major concern for the investment markets and Indian stock market is not an exception. Quality of decision is solely based on the information and its processing capabilities. Decisions are based on integrated information from all corners of life. Sharing of information is common in the efficient informative market. In the sharing information environment, authenticity and privacy of data requires more customized information security framework. Integrated model is requires to deal with the data in financial market. This paper introduces model of information security which deals with security issues of shared information of financial market with efficient data revocation in the cloud.

Security Model:

Cloud based integration of financial data are facing great challenges on various fronts. Various security models is being introduce but it need more customization to fit in the Indian financial market. In this paper we are introducing security model with the cloud based integrated data for the Indian stock market. Retention, identification and sustainability of ownership of the data in the cloud computing is the major cause of concern. In the broader green cloud model we show that ownership can't be transfer and owners are not agreeing to transfer its data. So, mechanism which integrates data by retention of ownership of the data will more applicable. Introduction of third party auditor is one of the mechanisms. In this mechanism, a new neutral third party will assigned after the consensus of all the owners and it plays a role of authenticator. It will also maintain confidentiality of data and user. In the online payment system, a role of middleware infrastructure providers are playing similar role to connect bank account. In this system, bank account details are kept confidential and transaction happens. In the stock market scenario, big data analytics will introduced and required to take forecasting decisions. In fig. 01, model of stock market data security with revocation of data in the cloud frame is being proposed. In this figure, heterogeneous and temporal big data is integrated and transfer to the cloud. Cloud server can responsible to maintain ownership table, security management protocols, authentication tools, analytical tools and existing cloud technologies like HDFS, Pig, Hive etc. This data can be transfer to the data after validation and verification of the third party auditor's clearance. To maintain security and ownership of the data, key based revocation methodology is come into play. Market regulators and all other users like intermediaries and investors have defined domain to excess data. This can be maintain and revoke by the key based revocation method. Analytical based tools in the cloud will help to generate customized reports for the decision making with the check by data revocation. There are more than 83, 000 intermediaries registered with the Indian stock market regulators. One of the major jobs of these intermediaries is to provide analytical data to the investors. All data can be provided in the big data environment with introduction of key based data revocation security model.

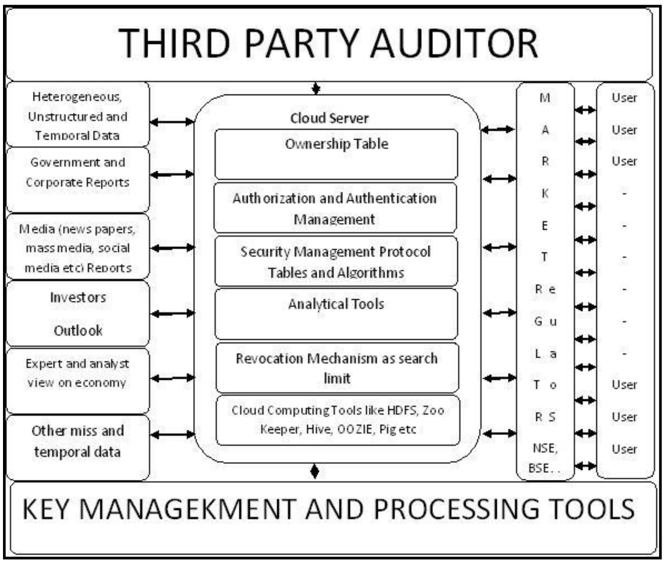
THIRD PARTY AUDITOR
Heterogeneous, Unstructured and Temporal Data
Government and Corporate Reports
Media (news papers, mass media, social media etc) Reports
Investors Outlook
Expert and analyst view on economy
Other miss and temporal data
Cloud Server
Ownership Table
Authorization and Authentication Management
Security Management Protocol Tables and Algorithms
Analytical Tools
Revocation Mechanism as search limit
Cloud Computing Tools like HDFS, Zoo Keeper, Hive, OOZIE, Pig etc
M A R K E T R e G u L a T o R S
NSE, BSE. .
User
User
User
-
-
-
-
-
-
User
User
User
KEY MANAGEKMENT AND PROCESSING TOOLS

Fig. 01: Revocation Model for Stock Market

In this green model, data from all walks of life which has capability to affect the market can be introduce by integration and provided through the cloud computing. Security introduction in the cloud model will generate confidence among investors.

Conclusion and Future work:

Forecasting of financial market behavior on the basis of cloud computing sharing data needs new framework under which privacy and authenticity must be protected. Proposed security model deals with the security and authenticity of cloud based data. Efficient handling of data revocation in the financial market's shared data will improved confidence level of the investors and other active players. Middle class population in the third world countries are untouched with the ups and down of the market directly. In the one hand they are victims of the price fluctuations in the market & its direct impact on their life's and on the other hand they have's confidence to participate in the market. Customized privacy framework will help to maintain the privacy of the user's personal data in the cloud. Data for the stock market has been integrating and became bigger and bigger. Forecasting requires all types of data like socio – economic – political as well personal to informative investment. More innovative and customized security framework is required to deals with the issues of information security in the stock market.

References

[1] Anders Fongen, "Identity Management without Revocation", DOI 10.1109/ SECURWARE.2010.20.

[2] Boyang Wang, Baochun Li and Hui Li, "Public Auditing for Shared Data with Efficient user

Revocation in the Cloud”, 978-1-4673-5946-7/13/$31.00 ©2013 IEEE.

[3] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou, “Identity-based Encryption with Outsourced Revocation in Cloud Computing”, Digital Object Indentifier 10.1109/ TC. 2013.208, 2013.

[4] Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang, “A Privacy-Preserving Scheme for Online Social Networks with Efficient Revocation”, proceeding IEEE INFOCOM 2010.

[5] Kan Yang, Xiaohua Jia, “Expressive, Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage”, Digital Object Indentifier 10.1109/TPDS.2013.253, 2013.

[6] Krishna Kumar Singh and Dr. Priti Dimri, “Integrative Information River Model For Financial Market’s Big Data Analytics”, International Journal of Applied Engineering Research, pp 35221-35225, Volume 10, Number 15, Sep. 2015.

[7] Krishna Kumar Singh, Dr. Priti Dimri and Madhu Rawat, “Green Data Base for Stock Market: A case study of Indian Stock Market”, IEEE Xplore digital library, pp. 848 – 853, DOI: 10.1109/CONFLUENCE.2014.6949306, 25 – 26, September 2014.

[8] Krishna Kumar Singh, Dr. Priti Dimri and J. N. Singh, “Green Data Base Management System for intermediaries of the Indian stock market”, IEEE Xplore digital library, pp. 1 - 5, ISBN number: 978-1-4799-3063-0, DOI: 10.1109/CSIBIG.2014. 7056996, March 2014.

[9] Krishna Kumar Singh, Dr. Priti Dimri, and Somitra Chakraborty, “Green Referential Data Base Management System for Indian Stock Market”, International Journal of Computer Application, Vol. 89(3), pp. 8 - 11, ISBN: 973-93-80880-18-3, DOI: 10.5120/15480-4197, March 2014.

[10] Ming Li, Shucheng Yu, NingCao, and Wenjing Lou, “Authorized Private Keyword Search over Encrypted Data in Cloud Computing”, DOI 10.1109/ICDCS.2011.55.

[11] RuWei Huang, Si Yu, Wei Zhuang, XiaoLin Gui, “Design of Privacy-Preserving Cloud Storage Framework”, DOI 10.1109/GCC.2010.36.

[12] Said Oulmakhzoune, Nora Cuppens-Boulahia, Frederic Cuppens, and Stephane Morucci, “Privacy policy preferences enforced by SPARQL Query Rewriting”, DOI 10.1109/ ARES. 2012.86, 2012.

[13] Shi-Cho Cha Kuan-Ju Huang Hsiang-Meng Chang, “An Efficient and Flexible Way to Protect Privacy in RFID Environment with Licenses”, 978-1-4244-1712-4/08/$25.00 ©2008 IEEE.

[14] Xiaohui Liang, XuLi, Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, “An Efficient and Secure user Revocation Scheme in Mobile Social Networks”, 978-1-4244-9268-8/11/$26.00 ©2011 IEEE.

[15] Xiaobiao Li, Qiaoyan Wen, “A Revocation Scheme for the Cloud Computing Environment”, 978-1-61284-204-2/11/$26.00 © 2011 IEEE.

[16] Yang Ming, Liu Fan, Han Jing-Li, Wang Zhao-Li, “An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control”, DOI 10.1109/IMCCC. 2011. 134, 2011.

[17] Yang Tang, Patrick P.C. Lee, John C.S. Lui, Radia Perlman, “Secure Overlay Cloud Storage with Access Control and Assured Deletion”, Digital Object Identifier no. 10.1109/ TDSC. 2012. 49.