IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 1, Feb-Mar, 2014
ISSN: 2320 - 8791
www.ijreat.org

Digitalised Secure Information Channel Maintenance in Distributed Brokering System

Roshni Kuruvilla[1], Ms.E.Thenmozhi[2]

Dept of CSE, Sathyabama University, Chennai

Abstract— Issues related for sharing information in a distributed system are the major practical issues consisting of autonomous entities which need to be securely transferred in a heterogeneous multi subdivided systems. Semi-honest nature of the intermediate brokers is taken as the base model for adversarial hacking or threats and a secure mechanism to safeguard the system is really wanted information for most of the business owners.

The end users are willing to share the information's/data secure across the network. Nevertheless, no individual entity will get exposed for the privacy reason. Consider a data is transferred from the user to the coordinators via brokers. In that case, there is a lot of possibility for data leakage and the intermediate people can hack the sensitive data of users. More possibilities are there for the attacker to infer some of the most important information's on the whole "user is interested in what, "where the user is, or something about the data of owner" , "infers which data server is having which data". To overcome this possible flaw of information's leakage, the existing system proposes a technique of encrypting here the entire data is with partial decryption technique to individual intermediate brokers.

Unfortunately, security mechanisms in validating the end to end users is missed out here and is trying to incorporate a digital signature based verification system which provides a highest secure data transmission through the channel.

Key words: semi honest nature, secure data transfer, digital signature

1. INTRODUCTION

A company or other organization that engages in the business of trading has several brokers through which the customers or clients can approach the company for shares. There are situation the brokers who act as an intermediate between the organization and the customers can change the quotation in order the gain money for their sake. The Preceding Limitation can be overcome by the novel based approach with the effective algorithms in order to overcome the problem of communication delimitation between company and customers.

The customers always wish that his data should be transferred in a secure manner from one destination to other destination through a network. Here the data is been transferred from the user to the coordinators through the brokers so there is a chance for the data leakage at the broker side. Here we take the semi honest nature of the brokers in the base system. For the secure data transfer we mainly use digital signatures so if the data is hacked then the whole data will become as an invalid one. Therefore the customer can assure that the data is been transferred.

2. RELATED ARTICLES

In the paper securing xml documents with the author-x written by Elisa Bertio and Silvana Castano in the year 2001explains the adoption of xml for the web based information exchange is having a flexible granularity in information retrieval. Xml can also define application specific document type by the use documents type definition. Here we mainly use a three-tier architecture for accessing the xml over the web and mainly it consist of web client ,network server and the back end information will be stored in suite of data sources here we mainly provide the user authentication by public key infrastructure but such mechanism for the excess control of documents contents or for their release and distribution.xml is mainly taken as an important scandalize tool for the secure transfer of information but her it supports the browsing and updating of DTD based xml sources. The highly secure of the web based service is not explained here.

In the paper Privacy Preserving Incremental Data Dissemination by Ji-Won Byun, Tiancheng Li, Elisa Bertino in the year 2006 uses K-anonymity and l-diversity model that led to a number of privacy-protecting techniques and algorithms this in turn will limits the static data release. An assumption is made that a complete dataset is available at the time of data release and this implies a significant short coming, as in many applications data collection is rather a continual process .This assumption entails "one-time" data dissemination ,hence it does not adequately address today's strong demand for immediate and up-to-date information . We consider incremental data dissemination, where a dataset is continuously incremented with new data. The key issue here is that the same data may be anonymized and published multiple times, each of the time in a deferent form. Investigation on the inference issues in more dynamic environments where deletions and updates of records are allowed is not discussed in this paper .And didn't consider all the inference issues only some of the specific items were considered in this.

In the paper Anonymity for continuous data publishing written by Benjamin C. M. Fung, KeWangy, AdaWai-Chee, Fux Jian Peiyin the year 2008 explains k-anonymization is an important privacy protection mechanism in data publishing.

While there has been a great deal of work in recent years, almost all considered a single static release. This mechanism only protects the data up to the release or recipient. In some practical applications, data is published continuously as new data arrive the same data may be used differently for a different purpose or a different recipient. In those scenarios, even when all releases are properly k-anonymized, the anonymity of an individual may be unintentionally compromised if recipient cross-examines all the releases received or colludes with other recipients. This paper mainly doesn't explain. Data with frequent changes like frequent updates / inserts were not considered in this paper and it add a major drawback in this paper. Due to dynamic environment, the frequent data releases make this project void.

In Mediated cipher text-policy attribute based encryption and its application, 10th international workshop by WISA in 2009 explains the Cipher text-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the cipher text is associated with an access policy over attributes. Here user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. Several CP-ABE schemes have been proposed, but some practical problems, such as attribute revocation, still need to be addressed. Here the author proposes a mediated Cipher text-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation. But possible extension to this work would be to provide a scheme which would have a security proof under standard complexity assumptions. This also leads to inefficient performance outrage.

In the year 2010 published a paper Improving privacy and security in multiauthority attribute-based encryption written by Melissa Chase, Sherman S.M.Chow tells Attribute based encryption determines decryption ability based on a user's attributes. For a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. This technique gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially un trusted authorities. But this system is more complex and the confidentiality depends critically on the security of the central authority. The methods and techniques used in this project are not efficient and do not contain all the security for the database.

3. SUMMARY OF EXISTING SYSTEM

In Regional Health Information Organization (RHIO) mainly have health providers a client and an intermediate to convey the details of the client to the doctor. So the client may not be interested to Conway the whole details about his deceases to the intermediate person. Same mechanism is been used in the information brokering system here v mainly have a client broker a coordinator who transfers the information to the particular company. Here in the existing system many information management applications and other sensitive information which we share with the broker parties and coordinators cannot be stored as a record of secured information.

And its security which is unconditional and does not depend on complicated computational assumptions when the invalid encryption takes place for the brokering control for data overlay. Moreover, the information management system should be robust such that it can still work when some distributed servers are corrupted and hided over the complex analysis. But this paper, we fail to focus on the most sophisticated and more wide range of applications for opting security providence by not allowing the broker agencies and coordinator parties to look into the unique authenticated information.

4. PROPOSED SYSTEM

In the proposed system we mainly concentrate the leakage of the data while transferring the data from the client to the coordinators via brokers. Here the system allows more complex data to be shared in a secured manner and it also has applications in privacy preserving data The problem of sharing privately is over come by our algorithmic approach by providing digital signature of the data, which cannot be identified by other parties extensively. The exertion reported in this paper further explores the modification of other parties between sharing secrets in an anonymous manner, will automatically make the original information to be an invalid one. By using the encryption standard our distributed secure computation system shows that our approach seamlessly integrates security enforcement at the user intensity with a certain trust level and accessing privilege providence of unified data access. Here we mainly use the digital signatures for securing the data while transferring here if the data is been leaked then it will be invalid by the formation of corruption.

5. BLOCK DIAGRAM

The diagram mainly explains working of the system

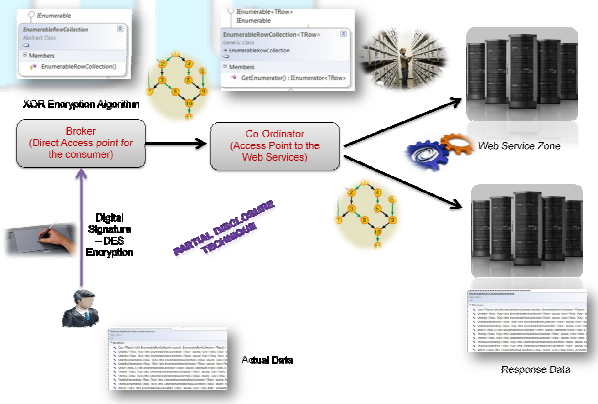

Fig 1.1 block diagram

Here the user mainly gives the details to the brokers and these data will be first encrypted and then digitally signed. So the information of the user will be completely hidden.

Next is the broker here the data will be completely hidden and the broker will get the user name only. Then it's the part of the coordinators for them by the help of the partial disclosure algorithm the user information like name and by whom they need share will be known to the coordinators and they will give the data to the particular share holders.

Then the web service zone mainly consist of the information of the company like its share cost quantity etc .When the user information is received to the particular company then the reply message is been received to the user .If the details are been hacked in between then the data will be completely invalid so no reply message will be received to the user so the particular user can understand his data is been hacked so therefore no loss o data will be there.

6. IMPLEMENTATION

This system mainly has phases like Data Utilization module, Digital signature zone, XML Signature verification zone, Partial disclosure co-ordination zone, Web Service zone.

Data Utilization Module

In this module, the data is in the form of request from the client to the organization is utilized. Client will easily buy the share for the certain company they like. The data regarding the share having the chances of getting in wrong hands like intermediate brokers. To overcome the problem the client data is organized in the way of encrypted format and utilized later by the certain techniques.

Digital signature zone

Digital signature is mainly an electronic signature that can be used to authenticate the identity of sender of a message or the signer of the document, and possibly for ensureing that the original content of the message or document that has been sent is not changed. In this module, all role players such as client, intermediates and the organization should authenticate the data using the procedure of digital signature. This digital signature format is an advanced techniques and safe way to transfer the data that is encrypted .By using this data some large quantity of data or detail got encrypted with the use of algorithm.

XML Signature verification zone

XML Signature defines the XML syntax for digital signatures. It is used reference validation and signature validation to validate the digital signature .In this module, the digitally signed documents by the client, intermediates and the organizations are validated in order to check its genuineness .Checking of the digital signature is main phase in the module.

Partial disclosure co-ordination zone

Partial disclosure co-ordination zone is mainly to safeguard the confidentiality between client and organization by preserving the data from the intermediates illegal activities. This module the data will be partially viewable according to the individual role players who acts as intermediate, this maintain confidentiality and direct dealing between client and organization .Even intermediates is not having the permission to view the data fully only the organization can decrypt the data and extract information sent by the client.

Web Service zone

Web services are an XML-based information exchange system that uses the Internet for direct application-to-application interaction. These systems can include the programs, objects, messages, or documents .In this module, the data from the client through intermediate persons are placed in a common place .The data's are then accessed by the organisation for providing further request .The decryption techniques are used effectively if there is any problem while decrypting the data cannot be extracted and in the certain organization may miss the exact data that wanted to be delivered.

7. PERFORMANCE EVALUATION

In this graph we mainly explain how efficient our proposed system than the existing system is .So by this we can clearly be able to know

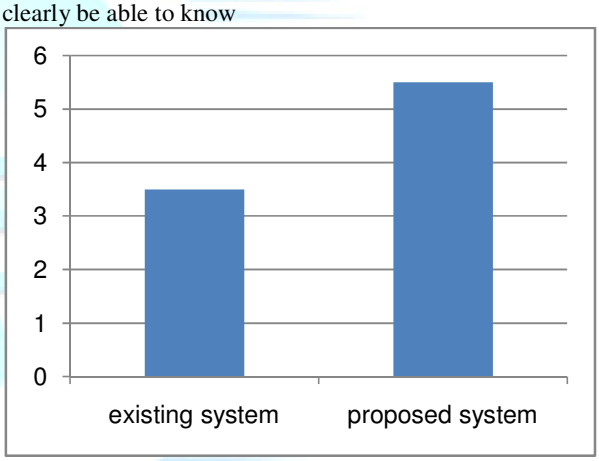

Fig 1.2 performance graph

the use of digital signatures the data is been transferred without any loss. So by the proposed system the security of the system is been assured.

8. CONCLUSION

While the data is been transferred from the user to the coordinators via brokers the data should be transferred in a secure manner. And also multiple data complex data should be transferred through the network. For the secure transfer we mainly use digital signatures for the encrypted data. Here the data can be transferred by preserving its privacy. Since we are using digital signatures if the data is been hacked then it will be an invalid one.

REFERENCE

[1] W. Bartschat, J. Burrington-Brown, S. Carey, J. Chen, S.Deming, and S. Durkin, "Surveying the RHIO landscape: A description of current {RHIO} models, with a focus on patient identification," *J. AHIMA*, vol. 77, pp. 64A–64D, Jan. 2006.

[2] P. Sheth and J. A. Larson, "Federated database systems for managing distributed, heterogeneous, and autonomous databases," *ACM Comput. Surveys (CSUR)*, vol. 22, no. 3, pp. 183–236, 1990.

[3] L. M.Haas, E. T. Lin, andM.A. Roth, "Data integration through database federation," *IBM Syst. J.*, vol. 41, no. 4, pp. 578–596, 2002.
[4] X. Zhang, J. Liu, B. Li, and T.-S. P. Yum, "Cool Streaming/.Net: A data-driven overlay network for efficient live media streaming," in*Proc. IEEE INFOCOM*,Miami, FL, USA, 2005, vol. 3, pp. 2102–2111.
[5] C. Snoeren, K. Conley, and D. K. Gifford, "Mesh-based content routing using XML," in *Proc. SOSP*, 2001, pp. 160–173. N.
[6] G. Koloniari and E. Pitoura, "Peer-to-peer management of XML data: Issues and research challenges," *SIGMOD Rec.*, vol. 34, no. 2, pp. 6–17, 2005.
[7] M. Franklin, A. Halevy, and D. Maier, "From databases to dataspaces: A new abstraction for information management," *SIGMOD Rec.*, vol. 34, no. 4, pp. 27–33, 2005.
[8] F. Li, B. Luo, P. Liu, D. Lee, P. Mitra,W. Lee, and C. Chu, "In-broker access control: Towards efficient end-to-end performance of information brokerage systems," in *Proc. IEEE SUTC*, Taichung, Taiwan, 2006, pp. 252–259.
[9] F. Li, B. Luo, P. Liu, D. Lee, and C.-H. Chu, "Automaton segmentation: A new approach to preserve privacy in XML information brokering,"in *Proc. ACM CCS'07*, 2007, pp. 508–518.
[10] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.
[11] R. Agrawal, A. Evfimivski, and R. Srikant, "Information sharing across private databases," in *Proc. 2003 ACM SIGMOD*, San Diego, CA, USA, 2003, pp. 86–97.
[12] M. Genesereth, A. Keller, and O.Duschka, "Informaster: An information integration system," in *Proc. SIGMOD*, Tucson, AZ, USA, 1997.
[13] Manolescu, D. Florescu, and D. Kossmann, "Answering XMLqueries on heterogeneous data sources," in *Proc. VLDB*, 2001, 241–250.
[14] J. Kang and J. F. Naughton, "On schemamatching with opaque column names and data values," in *Proc. SIGMOD*, 2003, pp. 205–216.