ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Xml Based Digitalized Secure Information Channel Maintenance in Distributed Broking Systems

S.Saravanakumar[1], M.N.Karuppusamy[2]

PG Student, Department of CSE, Sri Subramanya College of Engineering and Technology, Tamilnadu[1]

Research Scholar, Department of CSE, Sri Subramanya College of Engineering and Technology, Tamilnadu[2]

ABSTRACT: Issues related to sharing information in a distributed system is one of the major practical issues consisting of autonomous entities which needs to be securely transferred in a heterogeneous multi subdivided systems. Semi-honest nature of the intermediate brokers has been adopted as the base model for adversarial hacking or threats and a secure mechanism to safeguard the system is really a wanted information for most of the business owners. The end users are willing to share information's/secure data across the network. Nevertheless, no individual entity will get exposed due to privacy reason. Consider a data is navigated 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 the users. More possibilities are there for the attacker to infer some of the most important information's on the whole "who is interested in what" , "where who is, or something about the data owner" , "infers which data server has which data". To overcome the possible flaw of information's leakage, the existing system proposes a technique of encrypting the entire data with partial decryption technique to individual intermediate brokers. Unfortunately, security mechanism in validating the end to end users is missed out here and we are trying to incorporate a digital signature based verification system which provides a highest secure data transmission channel.

KEYWORDS: Distributed system, Brokers, Digtal signature or xml signature, Security

I. 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. To overcome this problem we introduce the technique Digital signature. In the digital signature there are two different types in it they are Bio-Metric signature and Data signature. In Bio-Metrics signature figure print, Eye recognition and thumb print will be presented. In Data signature Table signature and xml signature will presented. We are using the Data signature in that we using xml signature. In xml signature we using the RSA algorithm and single hash(#) technic.

II. PROBLEM

The 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 .The 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. The information management system must be robust such that it can still work when some distributed servers are corrupted and hided over the complex analysis. The author 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 .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

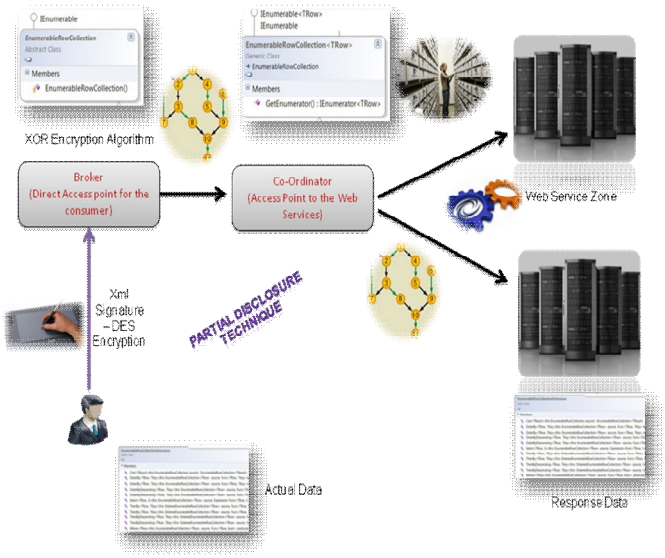
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III. ARCHITECTURE DIAGRAM



IV. TECHNIC USED TO IMPLEMENT

4.1 PARTIAL DISCLOSURE ALGORITHM

- Avoiding disclosure of sensitive info, which includes suppressing all sensitive entries in a table along with a specific number of other entries in the table, which in turn referred as complementary suppression.
- The idea is to allow each table entry x_i to be replaced by a convenient interval

  $[x_i - z- i , x_i + z+ i]$.
- The extreme values of each interval have then to be determined so as to ensure the required protection for the sensitive entries, while minimizing the overall loss of information incurred.

4.2 MD5 ALGORITHM

- Md5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted a, b, c and d. these are initialized to certain fixed constants.
- The main algorithm then operates on each 512-bit message block in turn, each block modifying the state.
- The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function f, modular addition, and left rotation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V. EXPERIMENTAL RESULTS

5.1 Data Utilization module:

Data in the form of request from the client to the organization is utilized. If the user is authenticated user then only it will be accessed and provide the authentication to the user to use the system.

5.2 Digital signature zone:

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. All role players such as client, intermediates and the organization should authenticate the data using the procedure of digital signature.

5.3 XML Signature verification zone:

XML Signature defines an XML syntax for digital signatures. It uses reference validation and signature validation to validate the digital signature.The digitally signed documents by the client, intermediates and the organisations are validated in order to check its genuineness.

5.4 Partial disclosure co-ordination zone:

Partial disclosure co-ordination zone is mainly to safeguard the confidentiality between client and organisation thereby preserving the data from the intermediates illegal activities.The data are partially viewable according to the individual role players who acts as intermediate, this maintain confidentiality and direct dealing between client and organisation.

5.5 Web service Zone:

Web services are XML-based information exchange systems that use the Internet for direct application-to-application interaction. These systems can include programs, objects, messages, or documents.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.

VI. CONCLUSION

6.1 SUMMARY:

The information brokering systems that exists suffer from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. we propose PPIB, a new approach to preserve privacy in XML information brokering. The quotation quoted by the user is sent through the brokers and corordinatiors to central web service zone where it is manipulated by the organizers. Intermediately to avoid the intrusion, the quotation is secured using the concept of digital signature.

6.2 FUTURE ENHANCEMENT:

Site distribution and load balancing in PPIB are conducted in an ad-hoc manner firstly. Next our research includes design an automatic scheme that does dynamic site distribution. Several factors can be considered in the scheme such as the workload at each peer, trust level of each peer, and privacy conflicts between automaton segments. And at the last we planned to minimize or eliminate the participation of the administrator node, who decides such issues as automaton segmentation granularity.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VII. ACKNOWLEDGEMENT

It is my pleasure to acknowledge Mr.J.Venkatesan Prabhu, Head, Kaashiv- InfoTech, Chennai for his support in implementation part and for his guidance throughout this course of work. And also wish to thanks our principal Mr. Babu Senathipathi and our staff Mr.M.Arul Prakash those who inspire me to write this paper.

REFERENCES

[1] Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu "Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 6, JUNE 2013

[2] 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.

[3] A. 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.

[4] 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.

[5] X. Zhang, J. Liu, B. Li, and T.-S. P. Yum, "CoolStreaming/DONet: A data-driven overlay network for efficient live media streaming," in Proc. IEEE INFOCOM,Miami, FL, USA, 2005, vol. 3, pp. 2102–2111.

[6] A. C. Snoeren, K. Conley, and D. K. Gifford, "Mesh-based content routing using XML," in Proc. SOSP, 2001, pp. 160–173.

[7] N. Koudas, M. Rabinovich, D. Srivastava, and T. Yu, "Routing XML queries," in Proc. ICDE'04, 2004, p. 844.

AUTHORS PROFILE

S.Saravanakumar was born in Oddanchatram in Dindigul District,Tamil Nadu, India in 1990. He got his Bachelor of Engineering in Computer Science and Engineering from Thirucharapalli Anna University, Thirchy in 2007. He doing his Master of Engineering in Computer Science and Engineering from Chennai Anna University, Chennai. His research interests areas are Web services, Computer Networks and Data Warehousing and Data Mining etc.

M.N.Karuppusamy was born in Dharapuram, Tamilnadu, India in 1984. He got his Bachelor of Science in Electronics from Bharathiar University, Coimbatore in 2005; He received his Master of Computer Application in 2008 from Bharathiar University, Coimbatore. He got his Master of Engineering in Department of Computer science and Engineering from Anna University - Coimbatore, Tamilnadu, India in 2011. Currently he is working as Assistant Professor in Department of Computer Science & Engineering, SSCET, Palani, India. His research interests are MANET, Network Protocol, Computer Networks, and Mobile Networks etc. He has published various national conferences related to Mobile Ad-hoc Networks for the past 3 years.