International Journal of Business Quantitative Economics and Applied Management Research
ISSN: 2349-5677
Volume 2, Issue 1, June 2015

Implementation of Secure Computing Methodology in Data Distributed System for Privacy Stabilization

Kalpana.B
Department of Computer Science and Engineering
Panimalar Institute of Technology
Chennai, India
Kalpanabalu1982@gmail.com

Abstract

Data Distribution plays a major role in the gigantically grown real time systems. Secure Computing Methodology is been proposed for the heavily grown data distributed system using an edge connection which takes care of the routing possibilities to guide the queries requested by the clients to the data server. Many of the existing systems visualize that the intermediators are trustable and they concentrate on the server point of view for confidentiality of data. But, the data consumption and location of data can be conditionally obtained from the Metadata's like Control rules, control queries which are in frequent exchange between the bound servers. All the current systems provide a very negligible concentration to privacy stabilization. In this paper, I have proposed an innovative methodology for secure computing in privacy stabilization. The two major attacks such as Quality relationship attack and Interpretation Attack are elaborated in detail first and two major solutions to the problems such as AUTOSEP (Automatic Separation) and ENCRPT O SEG (Encryption of Segment) are proposed to share the data securely among the group of servers. With the wide range of analysis I am going to show the approach when implemented provides excellent data stabilization for data distribution systems with low cost.

Index Terms – ***Data Sharing, Privacy and Data Distribution, Secure Computing Methodology.***

I. Introduction

There is a greater exploration of information collection in organization and in real time environments which are oscillating from many private sectors to business environments. There is a growing need for data distribution to provide privacy stabilization. Most of the existing systems concentrate on client server communication, information sharing and access control.

International Journal of Business Quantitative Economics and Applied Management Research
ISSN: 2349-5677
Volume 2, Issue 1, June 2015

But these models are not suitable for the gigantically growing data due to some mandatory reasons. In the context of practical sensitive and sensitive autonomous data, an easily adaptable solution is needed to make the routing decisions of data. Such a system can only be built with secure computing methodology. The following figure 1shows the overview of intermediator's and receivers.

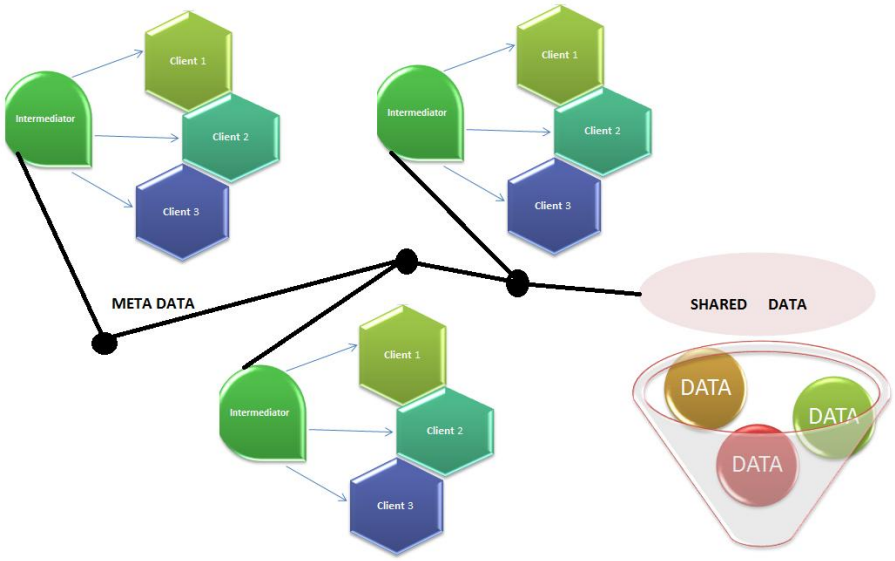

Figure 1: Overview of Intermediators and receivers

The data needed for the requested queries are subjected to multiple level checking and then it is forwarded to the central metadata server until it reaches to the destination server. This methodology is used for transparent and unified information services. The other information system services provide privacy and scalability but they are not completely reliable. It may be subjected to man in the middle attack, either by insiders or even by trusted outsiders.

In this paper I have given a unique solution for reservation of information and data. The methodology consist of two types of components namely ***intermediators*** and ***receivers*.** The intermediators are responsible for forwarding of the requested queries and user privacy checking. The receivers are used for providing routing of requested queries and to impose access control. They are used to provide scalability with significant transparency.

The paper is organized into sections such as problems and attacks in data distribution system (II), overview of solutions in data distributed system (III) and analysis of security and privacy (IV).

International Journal of Business Quantitative Economics and Applied Management Research
ISSN: 2349-5677
Volume 2, Issue 1, June 2015

II. Problems and Attacks in Data Distributed System

The two major attacks that normally occur in a data distributed system are quality relationship attack and interpretation attack. They are explained in the following sections.

- **Quality relationship attack**

All the requested query contents which include sensitive data cannot be easily handled or applied encryption because they are mandatory for routing of queries. In an important intermediators case there are three types of major share holders called owner, requester and servicer. Each of the share holders has their own privacy technique. The external attacker will have a silent man in the middle communication channel. Privacy issues will arise in case of very poor disclosure control.

The lower level intermediators learn about the content of queries and their respective location by means of using a local query methodology. Even if the data is well protected there will be still a case of eavesdropping. If the attacker finds the requested query with a heterogeneous expression and transfer the sensitive data about the owner such as passport number, pan card number, name in the credit card then this is called as quality relationship attack.

- **Interpretation attack**

In the current generation attack occur due to the location visibility of the user. Any person can be guessed by the location where he resides. The owner information is identity can be easily guessed from the IP address of is desktop are from his mobile phone GPS. Many privacy related information leakage occur when the outsider unnecessarily set sensitive information.

Moreover, with an implicit knowledge makes him easy for guessing. The outsider or the eavesdropper can readily obtain the scattered public data with is implicit knowledge. He can automatically create unnatural query and monitor the requested query and learns about the data distribution system silently for some period of time and can attack the location then there is a weak security of system. There are basically three types of sensitive information available for attack.

1. Data location and query location attack.
2. Query content attack
3. Data content attack.

International Journal of Business Quantitative Economics and Applied Management Research
ISSN: 2349-5677
Volume 2, Issue 1, June 2015

All these attack are concentrated on the targeting requester with specific location. The process of obtaining the data by the fact of guessing the users location is called as Interpretation attack.

III. Overview of Solutions in Data Distributed System

The receivers play a major role in routing of query and in the enforcement of access control with particular assumptions of preserving privacy. The server and the provider from heterogeneous organization will be able to communicate with each other by means of using intermediators. The *intermediators* play a vital role in providing interconnection between the receivers to enter or exit the system. This will help in analyzing the local logical traffic in the system. We cannot give the receivers complete freedom to rule the data but we can propose a methodology for implementation of secure computing in data distributed system by using AUTOSEP (AUTOmatic SEParation) and ENCRYPT O SEG (ENCRYPTion Of SEGment).

1. AUTOSEP (AUTOmatic SEParation)

The distributed data system and consortium of organizations will agree to share the data between them. Many organizations will come up with multiple methodologies but a global schema has to be followed for combining other local schemas. By doing so the control and index rules for all the listed organizations can be crafted by capturing of global phenomenon.

The basic idea of AUTOSEP is to divide the logically related data into independent data units and physically forward them to different intermediators for further use. The basic unit of a segment is called as AUTOSEP. The operation of the AUTOSEP can be done by storing each and every logical segment. Many segments can be given to the same intermediators by using port address and IP number which reduces the number of wanted intermediators.

After this operation implementation the intermediators can be logically linked and coordinated to their respective location in the segment and can derive themselves in the form of a tree structures. The intermediators when reaches the root of the tree behaves like a global automatic separator. When the intermediators travel through the root towards the leaves behaves like a local query and is called as leaf receivers. The automatic separation can be widely understood when duplication methodologies are known which is explained in the following sections.

International Journal of Business Quantitative Economics and Applied Management Research
ISSN: 2349-5677
Volume 2, Issue 1, June 2015

1.1 Duplication

Duplication plays a major role in data distribution systems. Multiple copies of data are saved extensively and used for further coordination among the receivers. All the requested queries undergoes the process of preprocessing when residing in the root, which in turn will lead to a performance bottle neck and ends up with single point of failure. Therefore duplication of root becomes mandatory for the tree to help in robustness.

1.2 Handling of duplication

The replication of data can be handled by matching the query against the index rules. When a query can read and access only the major subset of the data requested then it will be renamed to "XSAFE" before forwarding the remaining receivers, which makes the handling easy.

2. ENCRYPT O SEG (ENCRYPTion Of SEGment).

The encryption of segments will only take the XSAFE DATA for further communication. It is highly dangerous to hide a local query from inappropriate intermediators. However the traditional technique is not possible to implement in the real world for routing of query and access control. But the methodology which I have proposed called as AUTOSEP will provide a new door to encrypt even a atom of data and provide a true coordination between them.

When a critical query is encounter AUTOSEP can be applied using abstract methods. According to AUTOSEP methodology the segmented queries are processed and forwarding with a global key. The major challenge of this approach lies in the receiver association and in the settings available for data distributed system. To handle this problem we provide ENCRYPT O SEG uses private and public server key to avoid the major challenge.

International Journal of Business Quantitative Economics and Applied Management Research
ISSN: 2349-5677
Volume 2, Issue 1, June 2015

IV. Analysis of Security and Privacy in Data Distributed System

There are many kinds of attackers available in the data distribution system. These attackers can either be malicious insiders or trusted outsiders. We can categorize them according to the level of capabilities available. There are majorly three types of attacker's namely local eavesdropper, global eavesdropper and malicious intermediators.

- A local eaves dropper can transparently see all the available communication to and from the user level. He also has the capability of sniffing into outgoing and incoming private packets.
- A global use dropper is also a robust attacker who monitors the traffic and congestion in the network. But he cannot distinguish a data server from the receiver. He can just watch the gossips occurring between them and make a note of it logically.
- A malicious intermediators will disclose private information and important protocols to other organization. They can provide the location of the root coordinator and can end up with a threat to the network.

V. Conclusion

There is always a little amount of concentration given to privacy of data in distributed system. There are several factors that should be considered such as workload, trust, data distribution, conflicting data and balancing among data. This is an innovative separation policy which can be very easily applied to even a large system or organization. The methods like AUTOSEP and ENCRYPT O SEG provide considerable amount of privacy stabilization in secure computing. My next step of research is to design a scheme which can be directly applied to dynamic distributed data environment which will eliminate the unwanted interception of malicious attackers to the core and to make the methodology self reliable with robustness.

Acknowledgement

The author thanks Meghala Balu for timely and valuable support to complete the paper.

References

[1] 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 infor-mation brokerage systems," in *Proc. IEEE SUTC*, Taichung, Taiwan, 2006, pp. 252–259.

International Journal of Business Quantitative Economics and Applied Management Research
ISSN: 2349-5677
Volume 2, Issue 1, June 2015

[2] F. Li, B. Luo, P. Liu, D. Lee, and C.-H. Chu, "Automaton segmen-tation: A new approach to preserve privacy in XML information bro-kering," in *Proc. ACM CCS'07*, 2007, pp. 508–518.

[3]D. L. Chaum, "Untraceable electronic mail, return addresses, and dig-ital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[4]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.

[5]M. Genesereth, A. Keller, and O. Duschka, "Informaster: An informa-tion integration system," in *Proc. SIGMOD*, Tucson, AZ, USA, 1997.
[6]I. Manolescu, D. Florescu, and D. Kossmann, "Answering XML queries on heterogeneous data sources," in *Proc. VLDB*, 2001, pp. 241–250.

[7]. Kang and J. F. Naughton, "On schema matching with opaque column names and data values," in *Proc. SIGMOD*, 2003, pp. 205–216.

About The Author

Kalpana Balu received her Diploma Degree in Computer Science from Panimalar Polytechnic Chennai with First Class and Distinction with a Gold Medal affiliated to Directorate of Technical Education , B.Tech Degree in Information Technology stream from Sri Venkateswara College of Engineering, affiliated to University of madras and M.E Degree in Computer science and Engineering stream from Anna University, Chennai. She is an assistant professor in Computer Science and Engineering Department in Panimalar Institute of Technology affiliated to Anna University, Chennai. She has several high-level involvements in the area of Artificial Intelligence and Big data. Her areas of interest are Data Structures, Big data, Dependable and Secure Computing, Robotics and Data Distributed System. She has also published remarkable papers in the area of Dependable and Secure Computing. She has nearly 11 years of academic experience in the field of Engineering and guided many engineering projects.