ISSN 2229-5518

# A Review on Security Issues in Distributed Systems

Vijay Prakash, Manuj Darbari

**Abstract**— Development of secured and trusted distributed systems is a critical research issues. This paper is a contribution towards the summerization of work carried out in this field as well as identifies new research lines. Several approaches about security aspects in distributed systems have been discussed, like authentication based approaches, development of trust based models, access control based approaches, etc. A summarization of these issues is given in conclusion section. Apart from this, many research lines about secure distributed systems are discussed.

**Index Terms**—Distributed System Security, authentication, cryptography, quorum, mobile agent, trust based models, access control.

## 1 Introduction

The security techniques in distributed systems [1, 2, 44] are the important issues. Several elements of distributed system security are identified, like authentication, authorization, encryption and system protection. In initial days , the security management environment was based on single authority systems but now the focus is on the development of per activity, authorities and groups with shared responsibilities.

The general security attacks on the distributed systems are eavesdropping (gaining secret information), masquerading (making assumptions on the identity of users), and message tempering (changing the content of the message), replaying the message and denial of services.

The trustworthiness of distributed systems is important in a number of environments. For expressive economy the term security is used to represent both its traditional meaning as well as those notions carried by the term privacy.

Before discussing the factors affecting security in distributed systems, an overview of distributed system architecture is presented and used as a framework for subsequent analysis.

This paper has been divided into 3 secions. Section 2 explains various security aspects of distributed systems. Section 3 concludes the new research lines in developing secure distributed systems. Section 4 is conclusion and future scope.

## 2 Security Approaches in Distributed Systems

Various kinds of security approaches are used to make a secure distributed system. These are authentication based, trust based, access control based, cryptography techniques based etc.

### 2.1 Authentication Based Secuirty

A path authentication technique has been proposed in [1]. An on demand path discovery algorithm has been proposed to enable domains to securely discover paths in the collaboration environment.

A transport scheme for tracking the availability of entities in distributed systems has been proposed in [2].

Heterogeneous distributed systems are highly applicable in various applications, like electronic transaction processing systems, stock quote update systems which are requiring a highly efficient integration of authentication, integrity and confidentiality. A systematic security driven scheduling architecture has been designed in [3]. This technique has been proposed for DAG (Direct Acyclic Graph).The approach dynamically measures the trust of each node.

The authentication of remote client is an important research area in the distributed systems. A three factor based authentication approach for this purpose in [4]. In this, a two factor authentication has been extended to three factor authentication; it ensures the client privacy efficiently in distributed systems. The three factors used to develop this approach are, password, smart card and biometrics.

In [5], various aspects of the security in distributed systems has been given including, user authentication using passwords and digital certificates and confidentiality in data transmission.

The role of authentication servers in distributed computing systems has been discussed in [6].The main design issue are the cryptographic algorithms, synchronization and amount of trust.

A secured password based authentication with a trusted third party is developed in [7]. The approach is based on well-known authentication protocol, called KerberOS.

### 2.2 Trust Based Security Approaches

A trust based model has been developed in [16] for various applications, like P2P system.

Trust models are playing important role in the development of security systems in distributed applications. An extended D-S

- *Vijay Prakash is currently pursuingPh.D. from BBD University in Department of Computer Science & Engineering. He. is M. Tech. and M. Phil. E-mail:vijaylko@gmail.com*
- *Manuj Darbari is working as a Professor in the Department of Computer Science & Engineering in BBD Univerity, Lucknow, India. He is Ph. D. in Computer Science. He has published many papers at national and international level. E-mail: manujuma@gmail.com*

theory based trust model (ExDSTM) is developed in [17]. Other D-S theory models are proposed in [18, 19, 20].
A dynamic and context sensitive trust based security mechanism has been developed in [21].
A risk management has been integrated into security by using a trust model in [8].This model shows that the risk management can be applied to maximize the utilization of the distributed system. This model has the utility to evaluate the trust, also.

### 2.3 Access Control Based Security

A path authentication technique has been proposed in [1]. An on demand path discovery algorithm has been proposed to enable domains to securely discover paths in the collaboration environment.
A transport scheme for tracking the availability of entities in distributed systems has been proposed in [2].
Heterogeneous distributed systems are highly applicable in various applications, like electronic transaction processing systems, stock quote update systems which are requiring a highly efficient integration of authentication, integrity and confidentiality. A systematic security driven scheduling architecture has been designed in [3]. This technique has been proposed for DAG (Direct Acyclic Graph).The approach dynamically measures the trust of each node.
The authentication of remote client is an important research area in the distributed systems. A three factor based authentication approach for this purpose in [4]. In this, a two factor authentication has been extended to three factor authentication; it ensures the client privacy efficiently in distributed systems. The three factors used to develop this approach are, password, smart card and biometrics.
In [5], various aspects of the security in distributed systems has been given including, user authentication using passwords and digital certificates and confidentiality in data transmission.
The role of authentication servers in distributed computing systems has been discussed in [6].The main design issue are the cryptographic algorithms, synchronization and amount of trust.
A secured password based authentication with a trusted third party is developed in [7]. The approach is based on well-known authentication protocol, called KerberOS.

### 2.4 Cryptography Based Approaches

A framework of security in a distributed system mainly considering a device level system control has been proposed in [22]. Public key cryptography, software agents and XML binding technologies are considered for this approach.
The development of secure distributed systems uses various approaches, like Public Key Infrastructure (PKI) and Role Based Access Control (RBAC). In [23], RBAC approach has been used to develop authentication based on Public Key Certificates (PKC).

### 2.5 Policy Based Approaches

A policy based distributed system security mechanism has been developed in [24]. This framework provides modular security policies and independent of underlying system .This framework is based on domain-specific language for specification, verification and implementation of distributed system security policies.
The actual integration of security policies in distributed systems has been discussed in [25]. These security policies are manually configured and automatically enforced to the distributed system.

### 2.6 Pattern Based Security

Various types of security patterns for distributed system security are received in [26] .Various types of pattern based security methodologies are well discussed and their maturity and appropriateness are evaluated.

### 2.7 Quorum Based Security Systems

Quorum systems are highly applicable for solving the problem of data consistency in distributed fault-tolerant systems in [27], an Intrusion – Tolerance Quorum System [ITOS] of hybrid time model based on Trust Timely Computing Base (TTCB) has been proposed.
A role based access control model has been developed in [28]. The Role Ordering (RO) schedulers are introduced along with concurrency control based on significance of roles assigned to the transactions.

### 2.8 Other Security Based Approaches

A mobile agent based security model has been proposed in [29].This model explains and analyze the strength of security and various threats.
The ability of the system to detect the illegal behaviours and fight back in intrusion with counter measures is called self protection. A methodology for assessing, implementing and evaluating the self-protected system has been proposed in [30].
The efficient collaboration in between security and privacy for distributed system security has been discussed in [31].
The design of distributed security systems can be optimized. Genetic algorithm has been utilized for this purpose in [32].
A security heterogeneity approach for scheduling model in the distributed system has been developed in [33]. A novel heuristics scheduling algorithm has been proposed, which strives to maximize probability that all tasks are executed without any risk associated with attack.
In [34] XtremWeb architecture has been discussed which consists of computing functioning in a large scale distributed systems. The architecture of the system and parallel programming paradigms are discussed very well.
A proposal for secure transaction in mobile system based on delegate object model in [35].It focuses on the challenging issue of distributed nature in modern computer systems.
The RAIN technology is discussed in [36], which is a research collaboration between Caltech and NASA-JPL on distributed computing and data storage systems for future borne missions. Several proof of concept applications are developed: like, highly available web server, video server, distributed check pointing system.
Legal Information Flow (LIF) scheduler is proposed in [37] to synchronize transactions so as to prevent illegal information flows.

An approach for secure service discovery by employing and incremental progressive exposure approach has been developed in [38].

Building secure P2P file sharing system is an important research area. A powerful adversary model has been proposed in [39] for implementing a threat adaptive secure file sharing system.

An open authentication model based on CORBA security service specification has been proposed in [40].

The security of information transmission over networks in distributed system is considered in [41].

The secure functions in considering two models of non-repudiation protocols are discussed in [42], which are specified using the Markovian Process Algebra PEPA.

A model has been designed in [43], which provides support for distributed advanced workflow transactions. Such kinds of work are called transactions. Such kinds of work are called transactional work flow.

For the purpose of modelling security protocols in distributed systems UML2 have been utilized in [45].

## 3 Security Issues and Challenges

The secured implementation of distributed systems has been generated lot of critical issues. Some of these are as follows:

1. Identification of methodology which asseses the security level in any system
2. Monitoring of the system security
3. Development of security metrices
4. Integration of techniques, like Cryptography etc. for secure distributed data communication
5. Application of middle ware in distributed system security
6. Application of web services in security purpoases

## 3 Conclusions and Future Scope

Authentication, access control, cryptographic techniques, quorum based system, trust based models etc. are many developments towards the generation of secure and trusted distributed systems. Such type of issues are well briefed in TABLE – I.

In future the authors are keen to devlop the new and competitive approaches for the development of secured distribured systems.

TABLE – I
Summerization of various security aspects in distributed systems

| S. No. | Category | Focus | Reference |
|---|---|---|---|
| 1 | Authentication Based Approaches | Path authentication technique | [1] |
| | | Security driven scheduling architecture | [3] |
| | | Remote Client authentication | [4] |
| | | Passwords, digital certificates and confidentiality | [5,7] |
| | | Cryptography in authentication servers | [6, 22, 23] |
| 2 | Trust based security | Risk management | [8] |
| | | P2P System | [16] |
| | | Extended D-S theory based model | [17, 18, 19, 20] |
| | | Context sensitive trust model | [21] |
| 3 | Policy based security | Modular security policies | [24, 25] |
| 4 | Pattern based security | Security pattern for distributed systems | [26] |
| 5 | Quorum based security | Distributed fault tolerance system | [27] |
| 6 | Other techniques | Mobile agent based system | [29] |
| | | Genetic Algorithm based | [32] |
| | | X-Tron Web Architecture | [34] |
| | | RAIN Technology | [36] |
| | | LIF Schedular | [37] |

## References

[1] M. Shehab, A. Ghafoor, E. Bertino, Secure collaboration in a mediator free distributed environment, IEEE Transactions on Parallel and Distributed Systems, vol. 19, no.10, pp.1338-1351, 2010.

[2] S. Pallickara, J. Ekanayake, G. Fox, A scalable approach for the secure and authorized tracking of the availability of entities in distributed systems, IEEE International Parallel and distributed Processing symposium , pp. 1-10, 2007

[3] T. Xiaoyong, K. Li, Z. Zong, B. Veeravalli, A novel security-driven scheduling algorithms for precedence-constrained tasks in heterogeneous distributed systems, IEEE Transactions on Computers, vol 60, no.7, 2011, pp.1017-1029.

[4] X. Huang, Y. Xiang, A. Chonka, J. Zhou, R.H Deng, A generic framework for three factor authentication: Preserving security and

privacy in distributed systems, IEEE Transactions on Parallel and Distributed Systems, vol. 222, no.8 2011, pp.1390-1397.

[5] K. Vieira, A. Schulter, C. B. Westphall, C. M. Westphall, IT professional ,vol. 12 no. 4, 2010, 38-43.

[6] D. Gollmann, T. Beth, F. Damm, Authentication services in distributed systems, Computers and Security , vol. 12, no. 8, Dec.1993, pp.753-764.

[7] W. J. Seung, J. Souhan, Secure Password authentication for distributed computing, International Conference on Computational Intelligence and Security, 2006, vol.2, pp.1345-1350.

[8] C. Lin, V. Varadharajan, Trust based risk management for distributed system security-a new approach, First International Conference on Availability, Reliability and Security, 2006, ARES 2006.

[9] Y. Bai, On distributed system security, International Conference on Security Technology, 2008, 54-57.

[10] H. Koshutanski, A survey on distributed access control systems for web business process, International Journal of Network Security, vol 9, no.1, pp.61-69, July 2009.

[11] D. Chadwick, A. Oterko, E. Ball, Role base access control with X.509 attribute certificates, IEEE Internet Computing, 7(2), pp. 62-69, Mar/Apr. 2003.

[12] R. Oppliger, A. Grenlich, P. Trachsel, A distributed certificate management system(DCMS) supporting group based access control, in Proc. 15th IEEE annual computer security application conference (ACSAC'99) ,241-248,1999.

[13] K.Seamons, W. Winsbotough, Automated trust Negotiation Technical Report, Us Patent and Trade Mark office,2002,IBM Corporation, Patent application field Max7,200.

[14] W. Yao, Fidelis: A policy driven trust management framework in iTrust, LNCS 2692, pp. 301-314, Springer-Verlag, 2003.

[15] Blaze M, Feigonbaum. J., Ioannidis J., Keromyties, A.D., The role of trust management in distributed system security in secure internet programming: Security issues for mobile and distributed objects, Vitek and Nensen, Editors, 1999, Springer-Verlag, http://www.Dgpter.com/papers/networksec.pdf.

[16] H. Li, M. Singhal, Trust Management in distributed systems, Computer, vol. 40, no. 2 2007, pp. 45-53.

[17] L. Jiang, J. Xu, K. Zhang, A new evidential trust model for open distributed systems, Expert systems with applications,39(3),2012,3772-3782.

[18] L. D. Huang, G. Xue, X. L. He, H. L. Zhuang, A trust model based on evidence theory for P2P systems, Applied Mechanics and Materials, 20 (23), 2010, pp. 99-104.

[19] J. Wang, H. J. Sun, A new evidential trust model for open communities, Computer Standards and Open Interfaces, 31(5), pp.994-1001, 2009.

[20] B. Yu, M. P. Singh, An evidential model of distributed reputation management, First International Joint Conference on Automous Agents and Multiagent Systems, AAMAS, 2002

[21] Y. Ding, F. Liu, B. Tang, Context sensitive trust computing in distributed environments, Knowledge Based Systems, vol. 28, pp.105-114, 2012.

[22] Y. Xu, L. Korba, L. Wang, Q. Hao, W. Shen, S. Lang, A security framework for collaborative distributed system control at the device level, IEEE International Conference on Industrial Informatics, 2003, pp.192-198.

[23] W. Chang-Ji, W. Jian-Ping, D. Hai-Xin, Using attribute certificate to design role- based access control, 4th International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003, pp.216-218, 2003.

[24] H. Hamdi, M. Mosbah, A DSL framework for policy based security of distributed systems, 3rd IEEE International Conference on Secure Software Integration and Reliability Improvements, pp. 150-158, 2009.

[25] H. Hamdi, A. Bocehula, M. Mosbah, International Conference on Emerging security Information , systems and technologies 2007, pp.187-192.

[26] A. V. Uzunov, E. B. Fernandez, K. Falkner, Securing Distributed systems using patterns: a survey, Computers and Security ,in press, http://dx.doi,org/10.1016/j.cose.2012.04.005.

[27] H. Zhou, X. Meng, L. Zhang, X. Oiao, Quorum systems for intrusion tolerance based on trusted timely computing base, Journal of Systems, Engineering and Electronics, vol 21, no.1 pp.168-174,2010.

[28] E. Tomoya, T. Makoto, Con-currency control based on significance on roles; 11th International Conference on Parallel and Distributed Systems, vol. 1, pp.196-202.

[29] L. Qi, L. Yu, Mobile agent based security model for distributed system, 2001 IEEE International Conference on Systems, Man and Cybernetics, vol. 3, pp. 1754-1759, 2001.

[30] N. De Palma, D. Hagimont, F.Boyer, L. Broto, Self protection in a clustered distributed systems, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 2, 2012, pp. 330-336.

[31] S. S. Hau, P. A. Bonatti, F. Dengguo, B. Thuraisingham, Security and privacy in collaborative distributed systems, 29th Annual International Computer Software and Applications Conference, 2005 ,vol. 1.

[32] P. Bykoyy, Y. Pigovsky, V. Kochan, A. Sachenko, G. Morkowsy, S. Aksoy, Genetic algorithm implementation for distributed security systems optimization,2008 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications, pp.120-124, 2008.

[33] T. Xie, X. Qin, Performance evaluation of a new scheduling algorithm for distributed systems with security heterogeneity, Journal of Parallel and Distributed Computing, vol. 67, no.10, Oct. 2007, pp.1067-1081.

[34] F. Cappello, S. Ojilali, G.Fedak, T. Herault, F. Magniette, U. Nen, O. Lodygensky, Computing on large-scale distributed systems: Xtream web architecture, programming models, security, tests and convergence with grid, p2p computing and interaction with grid, 21(3),2005,417-437

[35] N. Shenbagavadivu,S. Usha Savithri ,Enhanced Information security in distributed mobile system based on delegate object model, Procedeia Engineering, vol. 30, 2012, pp. 774-781.

[36] V. Bohossian, C. C. Fan, P. S. Lemahieu, N. D. Riedel, L. Xu, J. Bnick, Computing in the RAIN : a reliable array of independent nodes, IEEE Transactions on Parallel and Distributed Systems, vol. 12, no.2, pp. 99-114, 2001.

[37] T. Enokido, M. Takizawa, A Legal Information Flow (LIF) scheduler for distributed systems, International Conference on Parallel and Distributed Systems, 2007, vol. 2, pp. 1-8, 2007.

[38] J. Y. Vhoi, Z. Y. Li, H. Y. Yaun, O. Song, Privacy protection in service discovery for large scale distributed computing systems, IEEE International Symposium on Parallel and Distributed Processing Workshops and Ph. D. Forum (IPDPSW), 2011, pp.1025-1032.

[39] R. T. Di Piero, L. V. Mancini, A. Mei, Towards threat adaptive dynamic fragment replication in large scale distributed systems, IEEE International Symposium on Parallel and distributed processing ,2007, pp. 1-2.

[40] K.-A. Chang, B.-R. Lee, T.-Y. Kim, Open authentication model supporting electronic commerce in distributed computing electronic commerce research, 2002, vol. 2, no.1-2, pp. 135-149.

[41] A.V. Bovoselov, V. E. Ansiperov, A. A. Nikitov, Information protection in distributed systems with the help of different layer protocols, Journal of Communications Technology and Electronics, vol. 52, no. 10, pp. 1133-1136, 2007.

[42] Y. Zhao, N. Thomas, Computing methods for efficient analysis of PEPA models of non-repudiation protocols, 15th International Conference on Parallel and Distributed Systems (ICPADS), 2009, pp. 821-827.

[43] V. I. Wietrzyk, M. Tajuzawa, M. A. Orgun, V. Varadharajann, A secure transaction environment for work flows in distributed systems, 8th International Conference on Parallel and Distributed Systems, 2001, 198-205.

[44] R. Anderson, Security engineering: a guide to building dependable distributed systems, Wiley, 2010.

[45] X. Zhou, A modelling approach using UML2 for security protocols in distributed systems, LNCS 2012, vol. 141, pp. 57-64.