ISSN 2278-7763

A New Framework of Distributed System Security Using DNA Cryptography and Trust Based Approach

Vijay Prakash, Manuj Darbari

[1]Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, E-mail: vijaylko@gmail.com, [2]Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, E-mail: manujuma@gmail.com

ABSTRACT

The development of new security frameworks for distributed system is a critical research issue. Trust management based security approaches are highly applicable in distributed system security. This is not requiring the need for resolving identities in the authorization decisions. Such approaches are also well expressing the restrictions and privileges. A new trust based security framework extended with cryptography approaches is proposed in this paper.

Keywords : Trust management, Cryptography, DNA cryptography.

1 INTRODUCTION

Distributed Systems have become highly applicable due to the advent of Internet. Several resources are indentified for such type of computing environment; CPU cycles, I/O bandwidth and memory. The security mechanisms are developed to handle all the resources available in the computing environment. The major characteristics of the distributed system are; concurrency of components, lack of global clock and independent failure of components. Apart from these issues some other major security issues [1, 2] includes; multiple autonomous components, not sharing of components by all users, several points of control and several points of failure.

In the distributed system, various components are sub divided into other sub components. The components are provided with the several interfaces enabling them to interact with each other. This system runs with multiple processes. Also these processes are extended on multiple process. The examples of the distributed system includes; Local Area Network and Intranet, Automated Teller Machine, Network, Internet/World Wide Web and mobile and ubiquitous computing. In the distributed systems, clients send request to the servers for accessing the data. Now, a security mechanism is required to hide the content of original message which are directly related to security and privacy and an authentication approach for identification of remote user. The new challenges of distributed systems security include the detail of service attack and mobile code security. The term 'trust' [3] can be defined as a requirement for making decision on communication with other entity. The quantification of trust is an important research issue. The value of trust on which the system may allow the interaction is another important research issue. In majority, the trust management can be divided into two kinds; **1.** Rule base system; **2.** Reputation system. In the rule based systems, the trust is considered as the role that entity plays. In this paper, a trust management based security frame work has been proposed for the distributed system.

2 TRUST MANAGEMENT

In a distributed trust management system [4-9]; formal rules are used to express the 'trust'. The rights are granted for the other system based on the rules in a user requesting system.

TABLE I Rule Based Distributed Trust Management Systems

Specification	Naming delegation policies
Implementation	Chain discovery certificates
Applications	PGP-PKI, AC, etc.

In a reputation based trust management system, it is tried to capture the psychological notion of trust. In this case, all the passed interactions are playing a big role in making a trust decisions. In a reputation system, the interaction and feedback is obtained by evaluated participants. The positive feedbacks provide enhancement in the reputation. The collective experience of all participants expresses the reputation of whole system.

TABLE II List of Ongoing Trust Based Projects

S. No.	Name of Project	Description	Reference
1.	Policy Maker	First example of trust management engine	[10]
2.	AWK	which processes the signed request which are embodied in the trust management system.	[11]
3.	Key Note		[12]
4.	REFEREE		[13]

ISSN 2278-7763

5.	Simple Public Key Infrastructure (SPKI)	It was developed for carrying out experimental work on Policy Maker. This was designed using credentials which directly authorize actions in place of subdividing the authorization task in the authentication and access control mechanism. This supports all programmability of assertions like, polices and credentials. This is standard format of authorization certificates.	[14]

3 PROPOSED WORK

We propose a model for distributed system security framework. This is a rule based approach for quantifying the trust which is further post – processed using the reputation approach (Fig. 1).

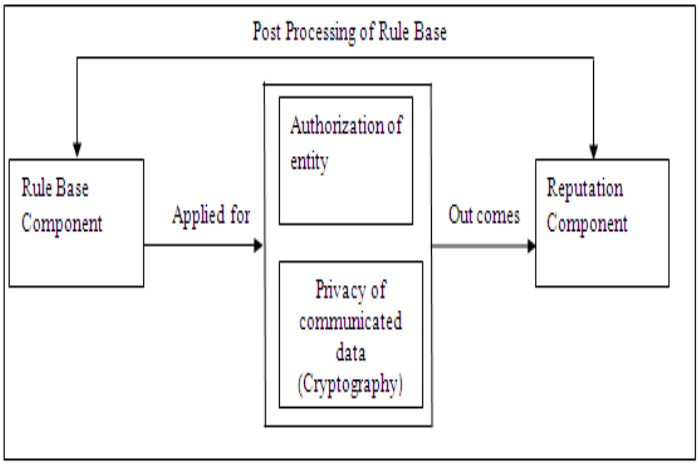

Fig. 1 Proposed Security Framework Based on Trust

In this framework, trust degree is the value obtained by the entity by the existing rule base. This is resented by 3 tuples {EID, TD, RF}

Here EID = Entity ID, TD = Trust Degree and RF = Reputation Factor.

Initially the TD is calculated by the rule Base which is updated by post processing using the following transfer function.

F: TD X RF ⟶ TD

Initially RF is equal to 1 and it ranges from 0 to 1 based on the calculation of reputation based approach.

Reputation component

In this proposed approach, the reputation component (Fig. 2) includes the following phases; Proof collection, Reputation Factor Approximation, Reputation confidence.

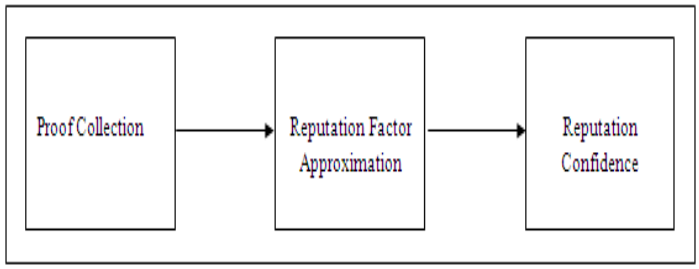

Fig. 2 Reputation component

As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap.

Reputation factor (RF) is represented by two tuples (RFV, RC) where RFV is the Reputation Factor Value raging from 0 to 1 & RC is the reputation confidence showing the authenticity of RF.

Rule based approach

Here, authors have used a DNA based cryptography [15] approach. The scheme is as follows:

In this approach the send message is encoded into binary. After that a random sequence is generated. A 4 point mutation is performed at binary plain text, now 8 point crossover operation is performed on the mutated B-Plain Text. The crossover mutated binary string is the Decrypted cipher text. In the Decryption approach, we perform Decrossover and Demutation operation using crossover key and mutation key. Decrossover is the reverse of crossover operation and demotion is the reverse of the mutation operation.

Procedure for encryption

The encryption approach is discussed in fig. 3 and 4.

ISSN 2278-7763

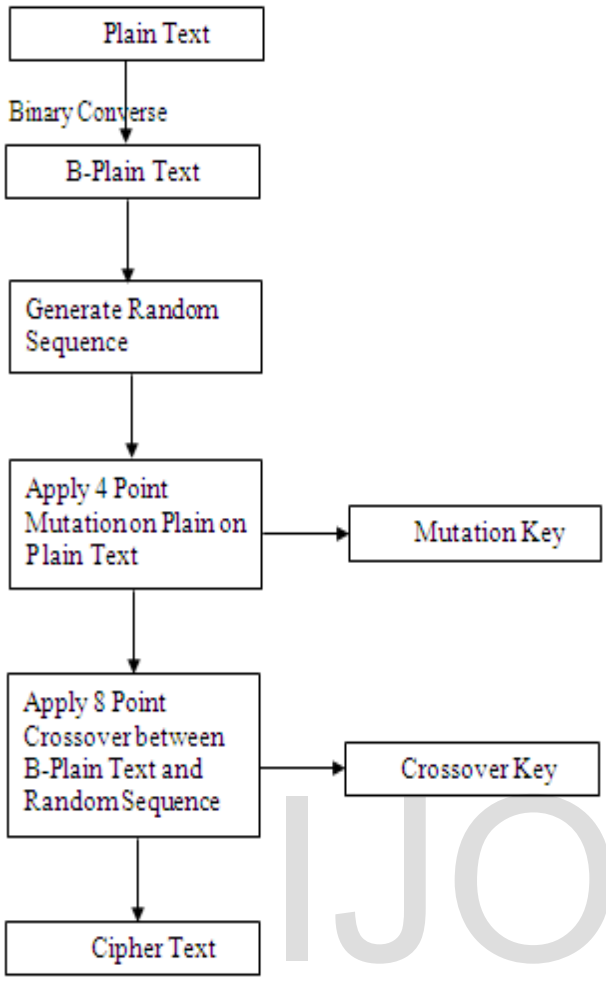

Fig. 3 Encryption operation

Procedure for decryption

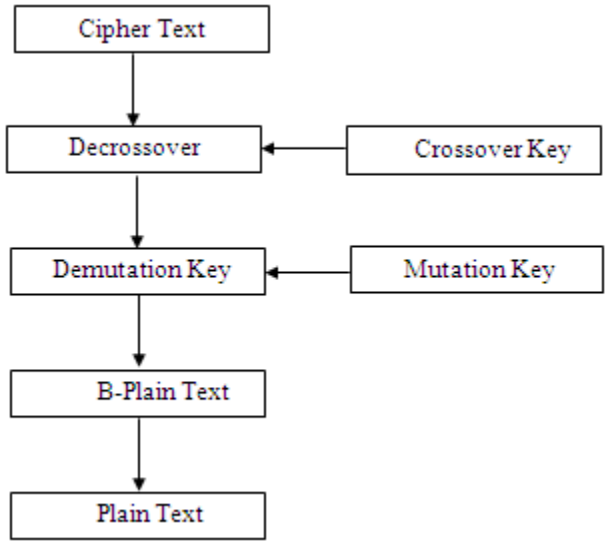

Fig. 4 Decryption operation

4 Experiments and Results

The experiments are carried out with the three approaches; approach 1 deals with the trust based system only, approach 2 deals with cryptographic approaches, approach 3 is the implementation of proposed approach. The experiment carries out the analysis of malicious node and trust value assessment.

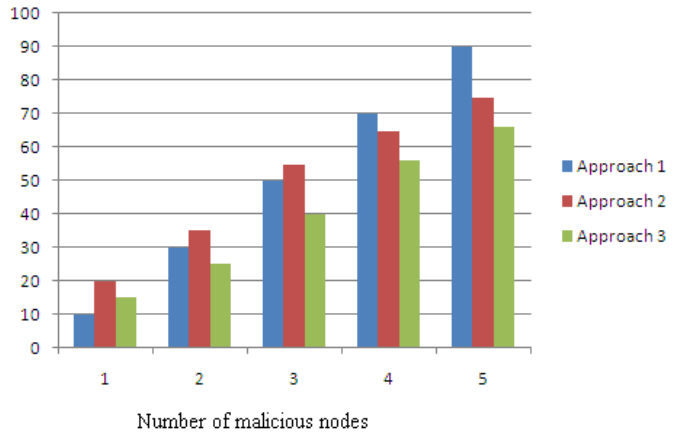

Fig. 5 Malicious Nodes Analysis

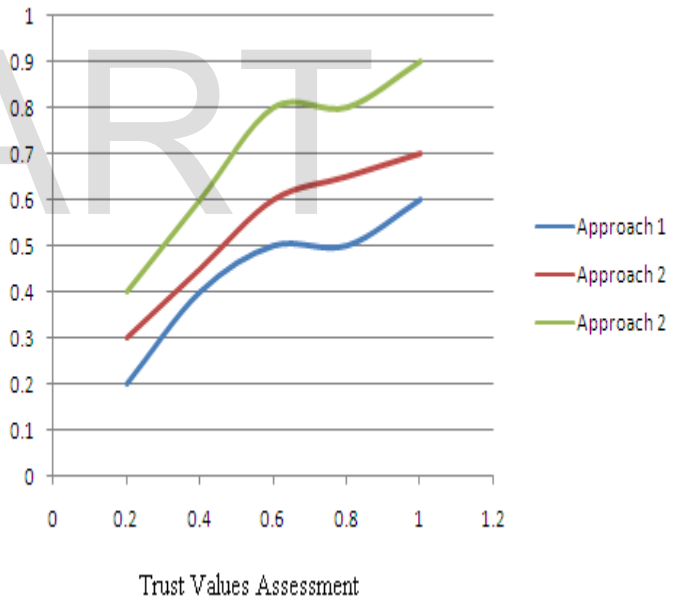

Fig. 6 Trust Value Analysis

5 Conclusions

Trust based distributed systems are the highly capable to deal with the security attacks in all aspects. The inclusion of cryptographic approaches is an excellent effort towards the development of more secure distributed systems. In this paper, the DNA based cryptography approach is integrated with a rule based post processing approach to deal with security attacks in the distributed systems. The experimental results are found competitive.

ISSN 2278-7763

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] 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.

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

[4] F.G. Marmol, G.M. Perez, Security threats scenarios in trust and reputation models for distributed systems, Computer and Security, Vol. 28, No. 7, Oct. 2009, pp.545-556.

[5] G. Schryen, M. Volkemer, S. Ries, S.M. Habib, A formal approach towards measuring trust in distributed systems, 2011 ACM Symposium on Applied Computing (SAC'11), pp.1739-1745.

[6] F.G. Marmol, G. M. Perez, Towards pre-standardization of trust and reputation models for distributed and heterogeneous system, Computer Standards and Interfaces, vol. 32 (4), June 2010, pp. 185-196.

[7] A. Aikebaier, T. Enokido, M. Takizawa, Trustworthy group making algorithm in distributed systems, Human Centric Computing and information Sciences, pp. 1-6, Nov. 2011.

[8] B. Zong, F. Xu, J. Pan, J. Lv, Comparing and evaluating collection strategizes in trust based reputation system in distributed environment, symposia and workshops on ubiquitous, Autonomic and Trusted Computing, 2009, pp. 557-562.

[9] W. Maiden, I. Dionoysiou, D. Frincke, G. Fink, D.E. Bakken, Dual Trust: A distributed trust model for swarn-based autonomic computing system, DPM 2010 and SETOP 2010, LNCS 6514, pp. 188-202, 2011.

[10] M. BLAZE, J. Feiginbaum, J.Lavy, Decentralized Trust Management. In Proc. Of 17th symposium security and Privacy, 164-173, IEEE computer society Press, Loss Alamitos, 1996.

[11] M. BLAZE, J. Feigembaum, J. Isonnidis, A. Keromyties, The keynote trust management system, http;//www.cis.upenn.edu/ angelos/keynote.html

[12] Y.-H.chu, J. Feiginbaum, B. Lamacchia, P. Beshick, M, straues, REFEREE: Trust management for web applications, World Wide Web Journal, 2, pp. 127-139, 1997.

[13] C.M. Ellison, B. Frants, R. Rivest, B.M. Thomas, T. Ylonen, Simple Public Key Certificate, http://www.pobox.com/cme/html/sphci.html.

[14] C.Lin, V.Varadharajan, Trust Based Risk management for distributed system security – a new approach, First International Conference on Availability, Reliability and Security (ARES06) pp. 2567-25670

[15] A. Gehari, T. Labean, J.Reif, DNA Based Cryptograph, Lecture Notes is Computer Science, Springer, 2004.

