CHAPTER 6

ENSURING DISTRIBUTED SYSTEM SECURITY USING DNA CRYPTOGRAPHY AND TRUST BASED METHOD

Distributed system security is well implemented by trust management systems. There is no need for resolving identities in the authorization decisions. These methods are well expressing the constraints and privileges. A new trust based security framework extended with cryptography approaches is implemented in this chapter.

6.1 INTRODUCTION

The applicability of distributed systems has been increased due to the advent of Internet. Multiple resources are designated for this type of computing environment; i.e. CPU cycles, I/O bandwidth and memory. The security approaches are introduced to deal with all the resources available in the computing environment. Main properties of the distributed system are; concurrency of components, lack of global clock and independent failure of components. Except these issues, some other major security issues (Shaheb et al. (2010), Xiaoyong et al. (2011)) includes; multiple autonomous components, not sharing of components by all users, several points of control and several points of failure.
Different components in distributed systems are sub-divided into other sub-components. The components are given with the multiple interfaces enabling them to communicate with each other. This system runs with multiple processes and these processes are extended on multiple processes. Local Area Network and Intranet, Automated Teller Machine, Network, Internet/World Wide Web and mobile and ubiquitous computing are different examples of distributed systems. Clients send request to the servers to access the data. A security mechanism is needed to hide the content of original message that are directly related to security and privacy. An authentication approach for identification of remote user has also been developed. The detail of service attack and mobile code security are the new challenges in the distributed system security. The term ‘trust’ proposed by Li and Singhal (2007) can be explained as a requirement for making decisions on communication with other entities. The approximation of trust is an important research line. The value of trust on which the system may allow the interaction is another important research issue. In majority, the trust management is divided into two types, namely rule base system and Reputation System. In the rule based systems, the trust is maintained as the role that entity plays.

6.2 TRUST MANAGEMENT

In a distributed trust management system (Marmol and Perez (2009), Schryen et al. (2011), Marmol and Perez (2010), Aikebaier et al. (2011), Zhong et al. (2009), Maiden et al. (2011)); ‘trust’ is represented by rules, the rights are granted for the other system based on the rules in a user requesting system.
Specification | Naming delegation policies
---|---
Implementation | Chain discovery certificates
Applications | PGP-PKI, AC, etc.

**TABLE 6.1 Rule Based Distributed Trust Management Systems**

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

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Name of Project</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Policy Maker AWK</td>
<td>First example of trust management engine which processes the signed request which are embodied in the trust management system.</td>
<td>Blaze <em>et al</em> (1996)</td>
</tr>
<tr>
<td>2.</td>
<td>Key Note</td>
<td>Implemented for carrying out experimental work on Policy Maker. Credentials are used for designing which directly authorize actions in place of subdividing the authorization task in the authentication and access control mechanisms.</td>
<td>Blaze (2014)</td>
</tr>
<tr>
<td>3.</td>
<td>REFEREE</td>
<td></td>
<td>Chu <em>et al</em> (1997)</td>
</tr>
<tr>
<td>4.</td>
<td>Simple Public Key</td>
<td>All programming of assertions like polices and credentials are</td>
<td></td>
</tr>
</tbody>
</table>
Infrastructure (SPKI) explained. This is standard format of authorization certificates. Ellison et al (2014)

<table>
<thead>
<tr>
<th>TABLE 6.2 List of ongoing trust based projects</th>
</tr>
</thead>
</table>

6.3 PROPOSED APPROACH

A model for distributed system security framework has been proposed. This is considered as a rule based approach for quantifying the trust values that is further post – processed with the help of the reputation approach.

![Proposed Security Framework Based on Trust](image)

Figure 6.1 Proposed Security Framework Based on Trust

Trust degree is the value obtained by the entity for the existing rule base as expressed in this framework. This is represented by 3 tuples \{EID, TD, RF\}.

Here, EID = Entity ID, TD = Trust Degree and RF = Reputation Factor.
At initial level, the TD is calculated by the rule base which is updated by post processing using the following transfer function.

\[ F: TD \rightarrow X RF \rightarrow TD \]

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

### 6.4 REPUTATION COMPONENT

The reputation component includes the following phases: proof collection, reputation factor approximation, reputation confidence as discussed below.

![Figure 6.2 Reputation Component](image)

Two tuples (RFV, RC) (Figure 6.2) are used for representing Reputation factor (RF) where RFV is the Reputation Factor Value ranging from 0 to 1 & RC is represented for reputation confidence showing the authenticity of RF.
6.5 RULE BASED APPROACH

DNA based cryptography approach has been developed by Gehari et al. (2004). The approach is as follows:

The encoding of send message is carried out into binary. Now a random sequence is produced. 4 point mutation is carried out 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 to cipher text. In the decryption method, Decrossover and Demutation operation are carried out using crossover key and mutation key. Decrossover is the reverse of crossover operation and demutation is the reverse of the mutation operation.

6.6 PROCEDURE FOR ENCRYPTION

The encryption approach is discussed in Fig. 6.3. In Encryption procedure the Plain text is converted into the B-Plain text with help of Binary converse, then this B-Plain text generates the random sequence, on this random sequence we apply the 4 point mutation on plain text with the help of mutation key after this mutation we apply the 8 point crossover between B-plain text and random sequence with the help of crossover key and after this we get finally the encoded text which is called as cipher text.
6.7 PROCEDURE FOR DECRYPTION

The Procedure for Decryption is illustrated in Fig. 6.4, in which the cipher text is converted into the decrossover with help of crossover key and after this with the help of mutation key is converted into demutation key, and after this cipher text is converted into the B-plain text and finally it converted into the Plain text i.e. the original text.
6.8 EXPERIMENTS & RESULTS

The calculation of Reputation Factor has been carried out using two important parameters, Reputation Factor and Reputation Confidence as discussed in section 6.4. The Mamdani FRBS has been used to implement and simulate a fuzzy system. The Block diagram is as follows:

![Mamdani Fuzzy System Diagram]

The membership functions of these input and output parameters are as follows:

![Member function of RF Diagram]
The following Figure 6.9 shows the generated rule base.
The procedure of inference engine values and text cases of accusing are as follows:

Wang Mendel Method has been used for the generation of rules which are further used in Rule Base for the purpose of inference engine settings.

Three kinds of approaches are used to carry out the experimentation. Approach 1 deals with the trust based system only, approach 2 deals with cryptographic approach; approach 3 is the implementation of proposed approach. The experiment carries out the analysis of malicious node and trust value assessment. The results are explained below.

![Figure 6.10 Malicious Nodes Analysis](image)
6.9 CONCLUSION

To deal with high risk security attacks in distributed systems trust based distributed systems are extremely applicable. Integration of cryptographic methods is an excellent effort towards the development of extremely secure distributed systems. The DNA based cryptography method is integrated with a rule based post processing method dealing with security attacks in the distributed systems.