5.1 INTRODUCTION

The previous chapters explained about the authentication manager of the trust based access control model. They described the process of detecting and preventing SQL injection and IP address spoofing. Authorization is the process of giving permission to someone to access the resource in computer. This chapter explains about the working procedure of authorization manager and its component called trust manager. In this access control model, authorization manager is responsible for granting or denying the permission to service requester who wants to access the service. Since this access control model granting or denying permission to web service requester based on their trust level, this access control model is called trust-based access control model.

Authorization manager has a component called as trust manager which evaluates the trust of each and every service requester who accesses the web service dynamically. It evaluates the trust value based on multifactors such as success rate, failure rate and access frequency, number of time out, average access time and server error. Thus, the service requester’s good behavior increases the trust value where as malicious actions or behavior will decrease the trust value and deny the access.

If the requester is good in success rate, access service frequently, and less in number of time out then their behavior is considered as good otherwise their behavior is considered as bad. The authorization manager invokes the trust manager, when access control rules defined in the access control policy are evaluated that needs the trust value of a web service requester.
5.2 TRUST MANAGER ARCHITECTURE

This section explains in detail about the working procedure of authorization manager and its component trust manager. Since the trust manager is the final process and takes the final decision on access permission, it plays an important role in the access control model.

The trust manager consists of trust management components such as Trust Decision Point (TDP), Trust Management Point (TMP), and Trust Negotiation Point (TNP) at service provider area. Since this trust management component is located separately in service provider place, it is easy to manage the trust value of requesters.

The architecture of the authorization manager is given in Figure 5.1 below. It has two components such as authorization manager and trust manager. These two modules are located in web service provider area. The next section describes the working procedure of all components in this architecture.

![Figure 5.1: Trust Manager Architecture](image-url)
The authorization manager will start its task once it receives the grant signal and user id from the authentication manager. Then, it calls the trust manager components by sending user id. The following section explains the working procedure of trust manager components and their interaction to calculate the trust value.

5.2.1. Trust Decision Point (TDP)

Trust decision point (TDP) is the first component of trust manager and it acts as interface between authorization manager and other trust manager components. Based on current trust value TDP takes initial decision of whether service requester allowed or denied to access the web services. In this model, the trust value ranges have been assigned from 0 to 10 and threshold value is zero. In the case of new requester, authorization manager assigns initial trust value of zero and calls TDP for decision. If the service requester is new to the system and access the web service first time, then TDP will not send request to calculate the trust value to TMP and TNP whereas it allows the service requester to avail the service from the provider and store the details of transaction.

If the registered requesters trust level is less than threshold trust value then requester will not be allowed to access the web services otherwise TDP sends present trust value to the TMP to calculate new trust value based on multifactor. After calculating new trust value, TMP gives the new value to the TDP. If the new trust value is greater than threshold value TDP sends grant permission to authorization manager otherwise it sends denial of access to the authorization manager. This initial trust level verification also makes system to consume less amount of time by avoiding calculation of trust level unnecessarily for the requester those who have trust value less than the threshold trust value.
5.2.2. Trust Management Point (TMP)

Trust management Point (TMP) is the second component of trust manager. The basic idea is that after the initial trust level verification done by TDP, Trust Management Point (TMP) evaluates trust value using the following factors.

1. **Success Rate named (St)** specifies number of successful transactions of a service requester in access control for a specified time period. This time period can be assumed by service provider.

2. **Failure Rate named (Ft)** specifies number of failure transactions of a service requester in access control for a specified time period.

3. **Frequency of Access (Af)** has the value of frequency of accessing the service by the requester. It has specified threshold value which can be assigned by service providers. If the requester’s Af is lower than threshold level, requester can be defined as inactive requester.

4. **Time-out named (To)** value specifies number of time-out occurs during resource access. This factor is used to recognize honesty of requester.

5. **Average Time named (At)**, Average time spent during service access in access control model. This factor also used to recognize honesty of requester.

This model is classified service requesters into four types according to their history of behavior in the system. They are 1.Honest and active 2.Honest and inactive 3.Dishonest and active 4.Dishonest and inactive.

Here is an example for the four types of user introduced above; if Time-out (To) and Average time (At) are less than its defined threshold value (Vo), then requester is considered as honest else dishonest requester.

If frequency of access (Af) is greater than its threshold level, then the requester is considered as an active requester, else inactive requester. Service provider
can assign their own threshold value for the above mentioned factors such as To, At and Af. They may assign the threshold value by considering factors such as requester numbers, network traffic etc.

Trust value calculation will be varying according to user’s type. The following section explains different types of users with their trust calculation formulae.

In the following formula, \( dt_{t+1} \) denotes new trust value at the time of \( t+1 \), \( dt_t \) denotes the present trust value at the time of \( t \). St denotes success rate, Ft denotes failure rate, Af denotes access frequency and Pf denotes penalty factor.

**Type 1:** If the requester is identified as honest and active, then requester’s decayed trust value \( (dt) \) will be increased as follows:

\[
dt_{t+1} = \frac{(dt_t + (St+Af)dt_t)}{(St+Ft)} \quad (1)
\]

For example, assume the values of Af=102; To=4; At=10; St=80; Ft=100; \( dt_t = 0.66 \); Also Consider, Af is greater than its threshold value and To, At are less than its threshold value. Since, user is honest and active the formula (1) is used to calculate the trust value. The values are applied in the formula (2) and obtained value is given below:

\[
dt_{t+1} = \frac{(0.66 + (80+102)*0.66)}{(80+100)} = 0.67
\]

According to the calculated value, it is concluded that trust value is increased for honest and active users.

**Type 2:** If the requester is identified as honest and inactive or dishonest and active, then requester’s decayed trust value \( (dt) \) will be decreased as follows:

\[
dt_{t+1} = \frac{(St+Af)dt_t - dt_t}{(St+Ft)} \quad (2)
\]

For example, assume the values of Af=90; To=4; At=10; St=80; Ft=100; \( dt_t = 0.66 \); Also Consider, Af is less than its threshold value and To, At are less than its threshold value. Since, the user is honest and inactive the formula (2) is used to
calculate the trust value. The values are applied in the formula (2) and obtained value is given below:

\[ dt^{t+1} = ((80+90) \times 0.66) - 0.66 / (80+100) = 0.62 \]

According to the calculated value, it is concluded that trust value is decreased for honest and inactive users.

**Type 3:** If the requester is identified as dishonest and inactive, then requester’s decayed trust value \( dt \) will be decreased by subtracting penalty factor as follows:

\[ dt^{t+1} = ((St+Af) \times dt^t) - dt^t / (St+Ft) - pf \]  

In the formula \( pf \) denotes penalty factor. According to Formula (3), it is concluded that trust value is decreased and penalty will be added for dishonest and inactive users. In the above formula, service provider can assign penalty factor. This system assumes penalty factor as 0.05.

For example, assume the values of \( Af=90; \ To=6; \ At=20; \ St=80; \ Ft=100; \ dt^t=0.66; \ Pf=0.5 \). Also Consider, \( Af \) is less than its threshold value and \( To, At \) are greater than its threshold value. Since, user is dishonest and inactive the formula (2) is used to calculate the trust value. The values are applied in the formula (2) and obtained value is given below:

\[ dt^{t+1} = ((80+90) \times 0.66) - 0.66 / (80+100) - 0.05 = 0.56 \]

According to the calculated value, it is concluded that trust value is decreased for dishonest and inactive users.

The above formulas and examples have explained trust value management in TMP. After calculating trust value, TMP checks for server failures during the previous transaction and user category. If there are server failures or user category is platinum then TMP sends request to TNP for negotiating the trust value so that honest users will not be punished.
The above formulas are derived from the basic direct trust calculation formula 
\[ T = \frac{S-F}{S+F} \]. After analyzing the basic formula, they are extended by adding multifactor such as Frequency of Access (Af) and Penalty Factor (Pf) to calculate trust value effectively. The algorithm for Trust Management Point (TMP) is given in following Figure 5.2.

\[
\text{dt} (St, Ft, Af, dt, To, At)
\{
\text{If (To>VTo and At> VAo and Af > VFo)} \quad \text{//User is honest and active}
\quad \text{Calculate } dt_{t+1} \text{ by using formulae (1)}
\}
\text{Else if (To>VTo and At> VAo and Af < VFo)} \quad \text{//User is honest and inactive}
\quad \text{Calculate } dt_{t+1} \text{ by using formulae (2)} \quad \text{// (or) dishonest and active}
\text{Else if (To<VTo and At< VAo and Af < VFo)} \quad \text{//User is dishonest and inactive}
\quad \text{Calculate } dt_{t+1} \text{ by using formulae (3)}
\}
\]

Figure 5.2: Algorithm for Trust Management Point (TMP)

In the above algorithm VTo, VAo and VFo are threshold values variables of Time out, Access Time and Frequency of Access time respectively.

5.2.3. Trust Negotiation Point (TNP)

TNP is the final process of trust manager where it negotiates the trust value of the eligible service requesters. TNP uses the following factors to negotiate the trust level.

1. **Server Error rate named (Se)** value is used in the trust negotiation point also to know about number of time-out or failure of request occurs due to server problem. Due to server error, sometimes the trust level of honest requester may be decreased or punished. To avoid this issue TNP checks the registered user database whether the previous service accesses has any communication failure due to server.
Then this kind of requesters' trust value can be negotiated. This factor is considered to avoid the penalty factor for honest and active users.

2. User class named (Uc) is used to identify the class of platinum user. In this access control model maximum trust value is defined as 10. For example, if user maintains trust level as 10 for one month then user class will be assumed as platinum user. This factor is used to reward the honest users.

So, if there is server error or user maintains platinum user class trust level TNP negotiates the value by adding Negotiate Factor (Nf) with the value send by the TMP. The formula for trust value negotiation is as follows:

\[ dt_{t+1} = dt_t + Nf \] (4)

In the above formula, \( dt_{t+1} \) denote new trust value at the time of \( t+1 \), \( dt_t \) is the newly computed trust value and \( Nf \) is the negotiation factor. Negotiation factor (Nf) is defined as 0.05 in this model.

For example, assume the values of \( Af=90; \ To=6; \ At=20; \ St=80; \ Ft=100; \ dt=0.66; \ Pf=0.5 \). Also Consider, \( Af \) is less than its threshold value and \( To, At \) are greater than its threshold value. Since, user is dishonest and inactive the formula (2) is used to calculate the trust value. The values are applied in the formula (2) and obtained value is given below:

\[ dt_{t+1} = \frac{(80+90)*0.66 - 0.66}{(80+100)} - 0.05 = 0.56 \]

According to the calculated value, it is concluded that trust value is decreased for dishonest and inactive users. In the above example, assume that server error is occurred in the last transaction. But requester is punished because of failure rate and time-out numbers of requester gets increased. Hence, TNP adds 0.05 with \( dt_{t+1} \) to negotiate the value as follows formula (4). Thus, \( dt_{t+1} = 0.56 + 0.05 = 0.61 \).
To avail negotiation process, platinum user class requesters should reach maximum value of 10 and maintain the same value for one month. Negotiation process will be negotiating honest and active users for three times to encourage their honesty and activeness.

In the algorithm Se, Uc and dt are variables of Server error, User class and decayed trust value at the time of t respectively. This algorithm describes about the negotiation process of trust value. It adds negotiate factor with trust value if there is server error or platinum user type. Otherwise, it returns the trust value without adding negotiate factor. The algorithm for Trust Negotiation Point (TNP) is given in the Figure 5.3.

```
dt (Se, Uc, dt)
{
    If server error or platinum user
        Add negotiate factor (Nf) with dt\textsuperscript{t+1}  // Negotiation factor is added.
        Return dt\textsuperscript{t+1} with adding negotiate factor (Nf)
    Else
        Return dt\textsuperscript{t+1} without adding negotiate factor (Nf)
}
```

**Figure 5.3: Algorithm for Trust Negotiation Point (TNP)**

Finally, the negotiated trust value will be sent to TDP through TMP. TDP gets new trust value and send it to authorization manager. If the trust value is greater than threshold value authorization manager allows the requester to access the web service otherwise deny the requesters from accessing the service. This negotiation process encourages honest and active user to participate effectively.
5.2.4. Web service (WS)

Web service is a target resource in this access control model. The whole components are working to secure the web service by detecting and preventing malicious attacks. To simulate the access control model, E-library web service was developed and tested successfully. Web service also responded well to the trusted service requester. The granularity of resources provided in the infrastructure is at the level of web services. Web services enable each participant organization to provide access to their internal functionality and data to other participants.

5.3 CONCLUSION

This chapter discussed the working procedure of authorization manager and its trust computation component called trust manager. Also the trust manager sub components such as Trust Decision Point (TDP), Trust Management Point (TMP) and Trust Negotiation Point (TNP) were explained in terms of calculating trust value of service requester. Also Trust manager describes the policy to allow accessing web services and trust manager calculates trust value of the user effectively.