3. TRUSTED CLOUD ATTESTATION MODEL

3.1 INTRODUCTION

Cloud is a disruptive technology where trusted cloud is the need of the hour to deliver services to meet the expectations of all the stakeholders. A consumer using public or private cloud service must rely on the provider for resources; in exchange, the provider must trust the consumer that the service delivered would be satisfactory in accordance with user’s requirements. Meanwhile, both, in turn, have to trust the software services for its behaviour and attack resistance. Therefore, achieving trust is paramount, that has been regarded as the most significant challenge in the cloud environment.

Surveys carried out in the previous chapter have clearly emphasized the need to classify the services and its providers, along with the consumers for trustworthiness based on thorough assessment of various qualities of services. Hence this chapter begins the discussion towards understanding the evidence needed for trusting the cloud entities and gives a complete view of the proposed model.

3.2 TRUST EVIDENCES

Trust requires consistent event-based actions which are stochastic in nature. Hence to be analyzed statistically, there needs to be a process for observations using evidence taken from all stakeholders. Apart from security and privacy being an integral part of establishing trust, other essential evidences considered for our TCAM for the foundation of trust characteristics are behaviour, compliance, relationship, transparency, and reputation. These trust evidences are depicted in Figure 3.1 and discussed along with its implications as follows.

- Behaviour monitoring is an essential parameter for a trustworthy system; on the contrary, misbehavior would create an untrusted environment. Evaluating good behaviour needs Quality of Service attributes related to trusted nature of the evaluating entities.
Figure 3.1: Cloud stakeholders and trust evidence

- **Compliance** with service level agreements for delivery of resources and compliance by the stakeholders to oblige to various regulations are essential trust objectives [61]. Enforcement of agreements and regulations ensures the cohesiveness of consumers and providers.

- **Transparency** through auditability ensures trustworthiness through the process of reassessing the defined attributes in a well-established transparent manner using a third party delegate [62]. The absence of transparency creates a sense of distrust among the stakeholders.

- **Relationship** between stakeholders ensures a good reputation index. Despite good relations, there are possibilities of collusion attack with a common interest to destabilize the business of their competitor.

- **Reputation** indicates quality, belief and a strong opinion that are derived from user’s experience with the service. An unreliable feedback can damage the reputation by producing a false trust score.
3.2.1 Trust relationship with stakeholders

Our proposed model takes into account of direct observation of the behaviour for the formation of cloud federation [63]. Direct trust relates to the experience of the agent for a particular entity based on regular observations. Indirect trust is about how through others, the information is passed or migrated. Through the indirect method, there is a possibility of any malicious information being passed and hence information may be uncertain.

The context of trust in the cloud ecosystem can be formulated as the relationship between the main players, namely, the user, and the provider. Let a user be represented as \( U \), and service provider as \( P \). \( S \) is the purpose (service) for which the user interacts with the provider and \( D \) is the steps taken by the provider to deliver the service. The process is mediated through the broker \( B \). Then the context of trust in the cloud may be expressed as in equation 3.1.

\[
CT = \langle U, P, S, D, B \rangle
\]  

(3.1)

A user \( U_i \) can make any request with purposes \( \{S_1, S_2, \ldots, S_n\} \) to the available providers, \( U_i \rightarrow B_{\{P_i, \ldots, P_n\}} \) and anyone can claim one or more services to the available providers, listed by the broker. The steps taken by the provider \( P_i \), to initiate and complete the process of service request \( U_i(S_i) \) is represented as \( P_i(D_i) \). Thus the context of trust to be assessed depends on how \( D_i \) of \( P_i \), is processed to achieve the goal of \( S_i \) to \( U_i \) through the help of broker \( B \), which is formulated as the pair in equation 3.2.

\[
CT = \langle U_i(S_i), P_i(D_i) \rangle_B
\]  

(3.2)

3.2.2 Context of trust with stakeholders

The needs for trusts between the entities are based on many contextual situations which are described in this section using the Figure 3.2. The context of trust clearly identifies the need for a relational assessment between the three key stakeholders using standard attributes to quantify our proposed TCAM model.
Figure 3.2: Context of trust between providers, users, and service

Service provider's trust with user $T(P_i \in U_i)$ is needed for security reasons because there is a possibility of user hijacking the virtual machine of the hosted service.

Similarly, the user needs to trust the provider $T(U_i \in P_i)$, for the belief that the privacy of data is not revealed and any feedback given to the service is truly assessed.

User’s trust with service $T(U_i \in S_i)$, is one of the primary trust value to be calculated because the code deployed at users machine can attack the firewall and steal sensitive information.

Service trusting the user $T(S_i \in U_i)$, is essential for reasons where the user machine may contain malware or viruses that can corrupt the service and make it non-functional. Therefore, the service needs to initially check the user’s system for security assessment like availability of crypto processors or firewall protection, etc.

Service providers trust with service $T(P_i \in S_i)$ and the service’s trust with the provider $T(S_i \in P_i)$, are highly coupled and hence the need to judge them, depends on the cloud vendor. Even though it may be a serious concern for vendor – provider relationship, our research scope focuses only on the broker’s perspective.
3.3 PROPOSED TRUSTED CLOUD ATTESTATION MODEL (TCAM)

Based on the above-discussed relationship between the cloud entities, our research focuses on developing a trustworthy cloud environment that is attested by an auditor and adaptive in nature. Existing works have either provided trust assessment or trust based compliance model based on subjective logic. Hence, the need for a complete end-to-end trust model supported with evidence, based on objective logic is proposed as a novel approach called Trusted Cloud Attestation Model (TCAM).

The TCAM has a layered approach in developing the adaptive trusted solution for cloud computing. It has three essential models.

1. Behaviour Trust Model (BTM)
2. Attestation Process Model (APM)
3. Cooperative Trust Model (CTM)

These models efficiently identify the trusted nature of the services through the flow of events depicted in Figure 3.3, which is explained below.

Figure 3.3: Trusted Cloud Attestation Model
Consider a cloud service being requested by a consumer (1), through a broker. The broker based on the requirements of the user’s request searches for a suitable service from various providers and selects one for provisioning (2). Before the service gets provisioned for deployment at the user’s desk, the broker assesses the device’s capability for various trust attributes. As soon as the service is initiated the BTM starts the job of behaviour assessment. During this process, the behaviour of the user’s past records and service’s QoS values are measured and monitored by the Behaviour Monitoring System (BMS) (3). The measurements are checked with the available data set present in the Trust Data Repository (TDR) (4a). The service and the users are assigned a valid trust score (4b).

The two entities, namely the cloud service and the cloud users who have been classified based on their trust score, are now sent to the attestation process model for a reassessment of the score (5). In this layer, the model again measures the same QoS attributes that have been done at the initial stage by BTM.

The attestation management system re-examines the values with that in the TDR, which was stored earlier by BTM (7a). Once the values of the entities are judged, they are given a certification using Attestation Process Model (APM) (7b). The attested entities are sent to a centralized trust repository, where the entities are placed in different zones (8).

Next, the cooperative trust model begins to assess the service provider’s trustworthiness by extracting the measurements from the TDR as well as fresh information from QoS. The strategic enforcement policy monitoring system of the CTM enforces various policies for trust, coalition, and imputation (10b). The trusted service providers are then sent to the common trusted zone (11). The trusted zone classifies the three entities and places them in an Adaptation Manager (AM) (12). The AM enforces various adaptation algorithms dynamically based on interactions and its resultant value for the entities to be within the trusted zones. Also, the AM advertises the trusted entities to the cloud providers (13) and cloud consumers (14) for better serviceability and availability.
The research, therefore, aims to provide trust using a three-stage approach with various strategies and policies. Moreover, the entire process of trust establishment progresses iteratively in a phased manner starting from attribute identification to adaptation.

3.3.1 Algorithm of TCAM

The computing model for trust establishment follows a governed objective by integrating various phases which is presented as an algorithm below. The phases of TCAM is visualized in Figure 3.4 depicts the flow of the proposed work. These phases identify and process the individual components of services for its integrity and effectiveness. The cloud broker responsible for the trust management has to collect and compare the pieces of evidence for a behaviour pattern and judge the nature of trusted service. The cloud auditor helps in establishing trust attestation. Hence our proposed model follows a stepwise approach in defining, evaluating and governing the trust values. The governing phase has a cyclic approach, where it iteratively performs attestation, cooperation, and adaptation. Any cases of deviations or williness to improve can be reexamined for performing the process again and having a new trust value through the computation process.

![Figure 3.4: Phases of Trusted Cloud Attestation Model](image)


**Algorithm 1: Evaluation and Computation Phases of TCAM**

Cloud User ($U_i$) request Service ($S_i$) from Provider ($P_i$) through Broker ($B_{Ui}$) {
Evaluate Trust for $S_i$ and $U_i$, Begin TCAM

**Phase 1: Trust Definition**

- Metrics_Identification: Identify_Evidences (behaviour, compliance, relationship, transparency, and reputation)
- Define SLA and Trust functions

- ∀ Evidences Identify_QoS_Attributes (Service QoS and Security QoS)
- Service QoS attributes (Availability, Accuracy, Configuration, Usability, Flexibility and Assurance)
- Security QoS attributes (Confidentiality, Authorization, Authentication, Certification, Audit Logs, IP Security)

**Phase 2: Trust Evaluation**

- Start Observation of Attributes using Evidence Measurement
- Initiate BTM

- Evaluate initial trust using TCC, TTSE and TTCE algorithm
- Assign Weightage using AHP on a scale of 0 to 9
  - if Consistency Ratio $< 0.1$ else re-evaluate the weights.
- Assign Trust Value between 0 to 1
- Store Trust Value at TDR

**Phase 3: Trust Computation**

- for time instance ($T_1$)

- Define Rejection_Condition for Trust Value
- Compute the Trust based on History of Trust
- Categorize Trust based on statistical quantification
- Classify into Revocable and Irrevocable Trust
Place the Trust Values in Trust Zones

\]
\]

**Phase 4: Trust Attestation**

\}
\}

after $T_1$ trigger Attestation Process through bot

Cloud Auditor define Attestation Requirements and Principles

\{

Perform verification through TCAP

If $\text{Measured Value} == \text{Benchmark Value}$

then certify

else inform deviation to AM

Store the Certificate in TDR and send to AM for adaptation

\}
\}

**Phase 5: Trust Cooperation**

\}
\}

for every Service Provider ($P_i$) ∈ Cloud Broker ($B_i$) perform

Strategic Enforcement Policy Monitoring System (SEPMS)

\{

initiate Trust Policy, Imputation Policy, and Coalition Policy

Prove Cooperative Game Theory for Grand Coalition

Individual rationality and Core

Assure equal payoff for cooperation

else penalize for non-cooperation

\}
\}

**Phase 6: Trust Adaptation**

\{

for all Trust Cases follow Adaptation Policy

Identify Change Detection

Perform Verification Analysis

Follow Adaptation Plan

\}
\}

Thus the phases of trust ensure that the measurements are properly assessed for deviation through the layered models of behaviour, attestation, and cooperation.
3.3.2 Quantification of trust attributes

Quantification of the resources for evaluating our target entities namely, the user, the service provider and the services offered, needs a strong metrics. These metrics are the key to trust judgments and forms the evidence of integrity measurement. This evidence should be measurable or observed properties which can offer reasonable information on the target entities. Evidence can be a chain of trust judgments about earlier runs or on trustees’ trusted entity. To express this, in a particular context in time $T_c$, a cloud user $C_c$ trusts a trustee’s attributes, $T_a$, to make a claim about a service $S$, which has, attributes $A$ with parameter value $P_v$. Then, when a specific assertion for a service $A(S, P_v)$ is made in a context $T_c$, $C_c$ believes in the claim as shown in the below expression.

$$E_v T(C_c, T_a, A(S, P_v), T_c) \land \text{madeBy}(A(S, P_v), T_a, T_c) \land \text{in}(T_c) \rightarrow \text{believe}(C_c, A(S, P_v)) \ (3.3)$$

Hence, in evidence-based trust, an attribute trusted by a trustee can also be trusted by a cloud user in a particular context. Since the attributes are the evidence, the quality of the attributes guarantees the quality of proof. Therefore the QoS attributes must be carefully selected. Several research surveys justify that QoS based trust evaluation mechanism is the most suitable and direct method to evaluate trust in the cloud [64]. However, the number of attributes that are considered are not sufficiently good enough or either insufficient to be considered as a valid model. Hence an approved and standardized measure must be adopted.

Our trust model adopts the standard measures defined by the Cloud Service Measurement Initiative Consortium (CSMIC). The Service Measurement Index (SMI) provides a list of quality attributes need for selection of cloud service providers [65]. The SMI constitutes seven categories namely accountability, agility, assurance, financial, performance, security and privacy, and usability. These categories are subdivided into multiple attributes with a set of Key Performance Indicator’s (KPI). These holistic views of indicators are modified accordingly to our trust evaluation.
Therefore, the SMI for our TCAM can be broadly classified as below.

- Service capability QoS attributes
- Security capability QoS attributes

Each has six attributes described through their parameters, which are based on their service and the context as listed in Table 3.1 and Table 3.2.

3.3.2.1 Service capability QoS attributes

The quality attributes that can assess the trusted nature of cloud entities must have certain capabilities to initiate and run the service in accordance with an agreement with the user's requirement. Hence the below table identifies various performance indicators.

<table>
<thead>
<tr>
<th>Table 3.1: Service capability QoS attributes for behavioural trust</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QoS attributes</strong></td>
</tr>
<tr>
<td>Availability</td>
</tr>
<tr>
<td>Accuracy</td>
</tr>
<tr>
<td>Configuration</td>
</tr>
<tr>
<td>Usability</td>
</tr>
<tr>
<td>Flexibility</td>
</tr>
<tr>
<td>Assurance</td>
</tr>
</tbody>
</table>

3.3.2.2 Security capability QoS attributes

The quality attributes to deal with not the only running status of the services, but also the security protection mechanisms as mentioned in Table 3.2. Hence for trust evaluation, six security attributes are considered.
Table 3.2: Security attributes for analyzing possibility of attacks

<table>
<thead>
<tr>
<th>Security Attributes</th>
<th>Parameters</th>
<th>Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Availability of TPM or other encryption</td>
<td>Possibility of tampering and attacks</td>
</tr>
<tr>
<td>Authorization</td>
<td>Avg. no. to times trying to access root</td>
<td>Attempt to access unauthorized services</td>
</tr>
<tr>
<td>Authentication</td>
<td>No. of failed login attempts or sign-in</td>
<td>No. of times credentials exceeded threshold</td>
</tr>
<tr>
<td>Certification</td>
<td>Any third-party certificates</td>
<td>Evidence and proof of behaviour</td>
</tr>
<tr>
<td>Audit logs</td>
<td>Abnormal timing of access</td>
<td>Simultaneous login at different locations</td>
</tr>
<tr>
<td>IP security</td>
<td>Abnormal IP address and proxy changing patterns</td>
<td>Check for IP spoofing attacks</td>
</tr>
</tbody>
</table>

Table 3.3: Trust attributes computed for TCAM

<table>
<thead>
<tr>
<th>Trust Attributes (TA)</th>
<th>Service provider (P)</th>
<th>Service (S)</th>
<th>User (U)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Accuracy</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Configuration</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Usability</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Flexibility</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Assurance</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Authorization</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Authentication</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Certification</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Audit logs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IP security</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 3.3 shows the trust attributes that are considered to evaluate the trust for TCAM. Now these attributes must be ranked based on a pair wise comparison method using AHP.
3.3.3 Ranking attributes based on AHP

Ranking of cloud attributes is one of the important features of the model. Since an attribute may have sub-attributes, it follows a hierarchical structure. Therefore, traditional weighted sum-based methods cannot be applied. Based on the quality of service requirement of the cloud entities and based on the significant features with its respective priority, a relative ranking system must be adopted for computation of trust score. Hence for a multi-attribute evaluation, a ranking mechanism based on Analytic Hierarchy Process (AHP) is used for computing the weights.

AHP combines the qualitative and quantitative analysis where it divides the complicated system into ordered hierarchy [66]. A matrix for judgment is constructed with consistency ration acceptable if less than 10%. Similarly, the relative ranking of all the cloud attributes is given by Eigenvector of the matrix. A pair-wise comparison matrix is constructed for representing the relative importance of each criterion. A relative importance is assigned as per AHP scale between [1 to 9] as shown in Table 3.4.

<table>
<thead>
<tr>
<th>Relative importance quality</th>
<th>AHP scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal importance/quality</td>
<td>1</td>
</tr>
<tr>
<td>Somewhat more important/better</td>
<td>3</td>
</tr>
<tr>
<td>Definitely more important/better</td>
<td>5</td>
</tr>
<tr>
<td>Much more important/better</td>
<td>7</td>
</tr>
<tr>
<td>Extremely more important/better</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 3.4: Relative importance value

Based on the relative importance value, the attributes of TCAM, construct, and compare each criterion, and convert them to a quantitative number as weightage factor in the range of 0 to 1.

3.4 SUMMARY

- In this chapter, the evidence and its attributes for direct evaluation are presented as the case for selecting trust based parameters, because a
wrong selection can derail the system’s trustworthiness. The selections of attributes are taken as per international standards, to provide a transparent approach for all the cloud stakeholders.

- A complete architecture of the proposed TCAM is elucidated with the flow of events. Algorithm for TCAM and its phases of execution are presented in this chapter which gives a complete picture of the trusted cloud environment.

- Selection of QoS parameters based on service and security has been discussed through its context. Moreover, the methodology adopted for parameter weightage using AHP has been described.