**Implementation Modules:**

1. **Mcknight’s Trust Model**
2. **Computational Trust Models**
3. **Context and Trusting Belief**
4. **Belief information and reputation Aggregation methods**

**Mcknight’s Trust Model:**

The social trust model, which guides the design of the computational model in this paper, was proposed by McKnight et al. after surveying more than 60 papers across a wide range of disciplines. It has been validated via empirical study. This model defines five conceptual trust types: trusting behavior, trusting intention, trusting belief, institution-based trust, and disposition to trust. *Trusting behavior* is an action that increases a truster's risk or makes the truster vulnerable to the trustee. *Trusting intention* indicates that a truster is willing to engage in trusting behaviors with the trustee. A trusting intention implies a trust decision and leads to a trusting behavior.

Two subtypes of trusting intention are:

**1.** Willingness to depend: the volitional preparedness to make oneself vulnerable to the trustee.

**2.** Subjective probability of depending.

**Computational Trust Models:**

The problem of establishing and maintaining dynamic trust has attracted many research efforts. One of the first attempts trying to formalize trust in computer science was made by Marsh. The model introduced the concepts widely used by other researchers such as context and situational trust. Many existing reputation models and security mechanisms rely on a social network structure . Propose an approach to extract reputation from the social network topology that encodes reputation information. Walter et al. propose a dynamic trust model for social networks, based on the concept of feedback centrality. The model, which enables computing trust between two disconnected nodes in the network through their neighbor nodes, is suitable for application to recommender systems. Lang proposes a trust model for access control in P2P networks, based on the assumption of transitivity of trust in social networks, where a simple mathematical model based on fuzzy set membership is used to calculate the trustworthiness of each node in a trust graph symbolizing interactions between network nodes.

**Context and Trusting Belief:**

**Context:** Trust is environment-specific . Both trusters concern and trustees' behavior vary from one situation to another. These situations are called contexts. A truster can specify the minimum trusting belief needed for a specific context. Direct experience information is maintained for each individual context to hasten belief updating. In this model, a truster has one integrity trust per trustee in all contexts. If a trustee disappoints a truster, the misbehavior lowers the truster's integrity belief in him. For integrity trust, contexts do not need to be distinguished.Competence trust is context-dependent. The fact that Bob is an excellent professor does not support to trust him as a chief. A representation is devised to identify the competence type and level needed in a context.

**Belief information and reputation Aggregation methods:**

Belief about a trustee's competence is context specific. A trustee's competence changes relatively slowly with time. Therefore, competence ratings assigned to her are viewed as samples drawn from a distribution with a steady mean and variance. Competence belief formation is formulated as a parameter estimation problem. Statistic methods are applied on the rating sequence to estimate the steady mean and variance, which are used as the belief value about the trustee's competence and the associated predictability.