ISSN: 2093-5374 / E-ISSN: 2093-5382

Trust Management in Heterogeneous Ubiquitous Environments

Haydeer MohamadAbbas[1*], Dr.S. Sreeja[2], Dr. Deepa Rajesh[3], Omer Muhsen[4], K. Rajashanmugam[5], Dr.S. Madhavi[6], and Abdusamiev Dilmurod Abdugani Ugli[7]

[1*]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. iu.tech.eng.haideralabdeli@gmail.com, https://orcid.org/0009-0006-2404-4456

[2]Department of Management Sciences, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India. sreeja1805@gmail.com, https://orcid.org/0009-0006-0166-4046

[3]Department of AMET Business School, AMET University, Kanathur, Tamil Nadu, India. deeparajesh@ametuniv.ac.in, https://orcid.org/0009-0008-9743-4791

[4]College of Engineering Technique, Al-Farahidi University, Baghdad, Iraq. omermuhsen@uoalfarahidi.edu.iq, https://orcid.org/0009-0005-9634-8232

[5]Assistant Professor, Department of MBA, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India. thelegendx005@gmail.com, https://orcid.org/0009-0009-4361-1155

[6]Professor, Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu India. madhavis@ksrct.ac.in, https://orcid.org/0000-0003-3218-533X

[7]Turan International University, Namangan, Uzbekistan. abdusamiyev1993@bk.ru, https://orcid.org/0009-0000-0934-5783

Received: June 24, 2025; Revised: August 06, 2025; Accepted: September 10, 2025; Published: September 30, 2025

Abstract

New technologies integrate multiple systems and service platforms into one coherent environment. The coherent environment now promotes multi-scenario smart device interaction, all in real time. The presence of mixed devices and systems creates computational trust and security issues. This stems from their multifunctional capabilities, different ownership structures, and different security and privacy rules. In addition, dynamic and decentralized communication systems introduce significant complexity. Trust Management serves as the basis for this complexity, encompassing security and reliability, privacy, and trust. There are trust mechanisms that rebuild our trust in a given system. Other systems are more proactive, and these are integrated systems with a focus on being pervasive and proactive. This research is considered Trust Management, primarily focusing on the principles of Mobility and Context variability. This report includes several theorems on trust, consisting of reputation systems, trust, and context and integration, that demonstrate the versatility of each approach in meeting the needs of decentralized systems. In addition, this review expands on

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 3 (September), pp. 560-576. DOI: *10.58346/JOWUA.2025.I3.034*

*Corresponding author: Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf of Al Diwaniyah, Al Diwaniyah, Iraq.

elements of trust building, identity, behavior trust, history, and context trust. It then covers in detail the evaluation and decision process for trust, and three adaptive learning systems that trust accurately over time.

Keywords: Trust Management, Ubiquitous Computing, Heterogeneous Environments, Trust Evaluation, Context-Awareness, Security, Privacy, Trust Models, Interoperability, Adaptive Systems.

1 Introduction

New forms of use cases for computing technologies made it possible for computing technologies to become a pervasive, even critical, part of daily life activities, daily use, and offered services. This allowed different and advanced mobile computing, smart sensors, smart appliances, and cloud services to merge into a single system often called a heterogeneous, ubiquitous computing environment (Suresha, 2019) that operates asynchronously across different contexts simultaneously. Over-integration and advancement of systems placed greater importance on critical trust and reliance (Ganesan et al., 2024) in the system and on seamless, safe, context-aware, and trustworthy interactions across systems. For smart systems that do not control and dictate user interactions, trust relationships are formed by smart governance (Mahmood et al., 2019) that controls the discretion, trust, and control a user has to the various eco systems and systems of disparate control entities.

Given the challenges posed by complex ecosystems, a multitude of adaptive and scalable trust models have been developed. These models aim to manage the unpredictability and volatility of heterogeneous systems, where entities can merge, demerge, or change their actions. For instance, consider the recently proposed trust model inspired by biological systems and based on evolutionary simulations for open multi-agent systems with highly variable performance (Mhetre et al., 2016). This trust model resembles an immune response and is best suited to adaptive, static trust models used in static systems (Moreau & Sinclair, 2024). Also, more recent proposals, such as Trust Mesh, leverage blockchain technology to build an immutable, secure, decentralized, and persistent trust architecture for IoT systems to satisfy scalability and change-resistance requirements in heterogeneous, pervasive environments (Aravind et al., 2023). These are indicators that trust is no longer a simple functional attribute. It is a dynamic, measurable entity that can be altered by various circumstantial and behavioral factors.

Although much attention has been given to 'technical resilience', new research underscores the need to incorporate the human-centered and social elements of trust system management frameworks. As previously outlined, trust is relational and derives from reputation, prior interactions, context, and the environment. To address this, some scholars have developed social interaction frameworks and explainable trust reasoning for system design. As one study suggested, social interaction dimensions enhance the interpretability and acceptance of trust decisions, particularly in user applications where 'transparent integration' is indispensable and interpretability is critical (Shelar et al., 2024). In addition, these systems rely on the user's location, identity, and other situational context to evaluate trust behavior historically, thereby enhancing intelligent, real-time, context-aware trust decision-making (Rangwala & Buyya, 2025). These systems mark a shift in trust from policy-driven, security-centric models that rely heavily on trust policies to more adaptive, client-centered models (Ghate & Roy, 2024).

Despite the importance of the issues outlined above, the problems remain mainly unsolved and outline the need for additional research. Issues related to the integration of heterogeneous, ubiquitous environments, such as the need for systems to interoperate with different computational trust frameworks and the real-time, dynamic adaptability of trust models, remain structurally extremely difficult to address and represent the most significant gaps. Responding with trust model equilibria and with novel models that escape fully computationally closed systems represent areas of research with high potential impact. Other critical gaps, such as the equilibria and dynamics of distributed trust in extremely large and decentralized networks of devices and the mechanisms for privacy-preserving trust assessments, require primarily novel computing frameworks. Addressing such trust and access problems, which are relevant to other research areas, is important for the research community and the policy and decision-making communities.

Key Contribution

- Created an all-inclusive trust computation framework that assimilates direct trust, indirect recommendations, and contextual information to render useable and precise trust evaluations in heterogeneous ubiquitous environments.
- Improved the quality of inputs related to trust assessment by formulating a systematic control over data acquisition and preprocessing that guarantees uniformity, accuracy, and compatability among the various data sources.
- Asserted robust self-adaptive models for trust assessment by incorporating network quality, device compatibility, as well as time of day, making the model less static and more responsive to real world changes.
- Designed a hierarchically scalable multi-dimensional trust management model to facilitate efficient trust aggregation, anomaly identification, and centralized control set policy application at different levels within a system.

This research aims to develop an adaptable, comprehensive trust management system for heterogeneous, ubiquitous environments. Multiple entities and systems simultaneously working on trust evaluation and trust updating remain perplexing challenges. Multi-layered and adaptable models of trust remain patchy and under-examined. Model context change analysis in the Literature Survey addresses this gap, along with the adapted model. In the Methodology section, a unique approach to trust evaluation is explained. Here, trust is computed from the user's stance, along with context, direct and indirect referrals, and interrelations, using a comprehensive, adaptable value system and data processing architecture. Graphic analysis in the Results and Discussion section demonstrates the model's operational effectiveness on performance-differentiated datasets. It visually depicts dynamically evolving trust scores as the primary focus across varying changes in trust components. The Conclusion summarizes the framework's implementation benefits, which facilitate greater precision, flexibility, and security in ubiquitous computing environments.

2 Literature Survey

Ongoing research focuses on managing trust in interactions among devices in heterogeneous, ubiquitous computing environments. In addition to this study, other works examine trust in dynamic environments and propose new methods for evaluating and adapting to it (Omonov et al., 2025).

There is a remarkable improvement in various GNNs (graph neural networks) developed for trust evaluation. Specifically, the multi-layer GNN utilized by TrustGuard (Rangwala & Buyya, 2025) clarifies the mechanisms of evaluating trust through professional oversight of spatiotemporal trust aggregation. TrustGuard enables managing the continuous transitions of trust and provides dynamic defenses against a range of attack models, which is a marked improvement over traditional trust-evaluation models in several scenarios (Veerappan, 2024).

TrustGNN (Chinnasamy, 2024) improves on the graph-based model by defining trust-propagation and trust-composition models based on social networks. TrustGNN achieves high trust prediction accuracy by developing configurable trust-propagation frameworks that value different trust pathways, a key requirement for heterogeneous networks that are relationally and contextually adaptive (Malhotra & Joshi, 2025).

A major trust model which considers privacy and resiliency issues in open multi-agent systems has been developed (Anto Lourdu Xavier Raj & Mario Macrina, 2021). This focuses on self-stored trust and self-evaluation which makes trust adaptation to different performance levels and mobility easier and less communicative. Strengthened privacy and reduced communicative needs enhance resiliency which is important in ubiquitous computing (Sethi & Jain, 2024). Advanced multi-agent systems, such as those using blockchain technology, serve as an unmatched solution. TrustMesh (Lygizou & Kalles, 2025) uses a blockchain integrated framework to achieve Byzantine fault tolerance in distributed IoT systems (Wang et al., 2024). TrustMesh solves the problems of large distributed systems on trust (Pavleska, 2025; Lygizou & Kalles, 2025) through a unique consensus and a permissioned blockchain which provides security and efficient resource allocation thereby tackling trust issues in large distributed systems (Pavleska, 2025; Lygizou & Kalles, 2025). As the last note, in trust management, the idea of coupling it with access control has been introduced to secure environments with high uncertainty. The trust-based access control model (Goecks & Mynatt, 2002) dynamically and intelligently adjusts access based on contextual data and trust evaluation systems. The model promotes seamless, secure access control, which is important in pervasive environments where computing devices and their contexts are continuously changing.

3 Methodology

This section describes how trust is managed in different environments. In these environments, trust is managed based on the data collected from interactions with other systems. The approach discussed in the first chapter accounted for complete data collection, comprehensive data preprocessing, and a mathematical trust calculation model that incorporates direct interactions and recommendations. To address the ever-changing and varied complexities of pervasive systems, the designed system architecture and operational flow were built with built-in flexibility, scalability, and strong security.

3.1 Data Collection and Preprocessing

The precision of a trust management system depends greatly on the type and diversity of available data. In diverse and widespread situations, the number of data sources increases substantially, encompassing device and user engagements, contextual data about the immediate surroundings, and the trustworthiness of other sources.

Data Sources

During the data gathering phase, multiple key information types are obtained:

- Interaction or Transactional Data: This is the record of communication or transaction of any kind. It could be qualitative or quantitative. Each communication or transaction record indicates whether the interaction was successful, how long it took to receive a response, and how often the agent was contacted. For smart home interaction data, it will also include user activity logs and signals, from user command windows to sensor triggers.

- Trustworthiness Data: Trustworthiness considers Data is collected, per context. Geography, time of day, device attributes, and even network rete attributes, such as latency and bandwidth, are contextual factors for trust. Environmental attributes such as temperature or motion detection are also context.
- Trustworthiness Based on Data: Data based on trust is collected, based only on receiving feedback or ratings from a third party. This is particularly useful when establishing trust, especially if the conditions are rapidly changing and the context involves tier areas or people with little to no interaction.
- Social Networks Interaction Profiles: An actor's social network emerges from a combination of interaction logs and telemetry data, collected and stored over periods of time.

Preprocessing Steps

Various systems and devices generate raw data, and it is reasonable to expect that data will be inconsistent and incomplete. To provide a trustworthy outcome, trust models will need to integrate necessary processing or cleaning actions to ensure that the data is sufficiently trustworthy once verified.

- The Value of Trustworthiness that is Based on Data: This approach cleans and organizes trustworthy data by identifying invalid, duplicated or corrupted records. Missing data may need to be imputed or removed based on the relevance of the data set.
- Noise Filtering: Basic methods such as moving averages can smooth out data and remove outliers, as well as more complex machine learning filters such as the Kalman filter.
- Normalization: Data attributes captured from separate databases need to be normalized to a common range or unit. For instance, latency may be measured in milliseconds, whereas humans rate from 1 to 5. To maintain all data and describe the outcomes of actions at a higher level of aggregation, features can be normalized to a common bound, mapping 0 to 1.
- Feature Extraction: From complex raw data features that define trust are derived such as how often users interacted within a given timeframe, how they rated one another in a given time, and ranking the similarity of users' devices.

3.2 Trust Computation Model

In a data acquisition and preprocessing, earn-trust models for each entity in a heterogeneous, ubiquitous environment dynamically assess the trustworthiness of each entity. In evaluating trust within complex environments, reliance is placed on the three constituents of trust: direct trust from personal interaction, indirect trust from word of mouth, and contextual trust from circumstantial elements. Trust value is computed from three constituents: direct experience, social proof, and contextual considerations.

The overall trust T_ij)t) from entity i to entity j at a given time t is given as:

$$T_{ij}\ (t) = \alpha . D_{ij}(t) + \beta . R_{ij}(t) + \Upsilon . C_{ij}(t) \qquad (1)$$

Where $D_{ij}\ (t)$is the direct trust, $R_{ij}(t)$ is the indirect trust, and $C_{ij}(t)$ is the contextual trust. The weighting parameters α, β, γ are non-negative and satisfy α + β + γ = 1, allowing for a flexible emphasis on each trust dimension depending on the environment. These components and weights combine as shown in Equation (1) to calculate the overall trust value $T_{ij}\ (t)$.

Direct trust quantifies reliability based on past direct interactions, incorporating recency by applying an exponential decay weight ( ),$wk = e$^ $(- \lambda\ (t - t$_$k))$,to each interaction rating T_k. This weighting reduces the influence of older interactions, ensuring trust reflects recent behavior more heavily. The direct trust value is computed as a weighted average:

$$D_{ij}(t) = \frac{\sum_{k=1}^{n} w_k.T_k}{\sum_{k=1}^{n} w_k} \quad (2)$$

Here, λ > 0controls the decay rate, is the timestamp of interaction k, and $T_k \in [0,1]$ is the rating of that interaction, as defined in Equation (2).

3.3 Contextual Trust Computation

In past experiences and recommendations, trust is influenced in a broad context ubiquitous setting. Unlike other forms of trust, 'Contextual Trust' value captures the captured dynamic factors of all interactions that impact the multi-dimensional elements that is interface based which enables to interact with automation system on the environment with immense factors that are critical to trust as the level of trust can be different based on location, conditions and time.

Trust in contextual elements identifies applicable boundaries for consideration of settings where users' visibility and participation in automation processes occur. Physical proximity, device cooperation, network parameters, and time are among these parameters. Set criteria increase trust around devices that are situated close together or on the same Ethernet segment. Devices running the same operating system tend to work together more effectively than those with different configurations, thereby enhancing cooperation.

Considering quality of the connection is yet another context/criteria that must be taken into account. Low-latency, stable connections, and high-bandwidth connections promote seamless communication, which, in turn, fosters growing trust. Conversely, poor connections undermine trust due to delays, information loss, and disruptions in continuity. There are also time issues; trust can depend on time of day or business hours, as entities are known to operate and behave differently outside of business hours.

In trust calculations, the contextual trust calculation process involves retrieving specific features. Relevant contextual components are selected and weighted based on the surrounding context. Here, the trust model adapts to the contextual needs, focusing more on factors that support trust for that particular application or system in use, as outlined in the designed trust model. Each weight is assigned a value based on the field's competencies and further refined with historical data and algorithms based on computational learning.

Real-time adjustments made on the basis of contextual information adaptation help manage the systems trust issues have. This increases responsiveness of the interacting entities to their surroundings, assisting in the formation of trust metrics that swiftly adapt to changes in the situation. This type of automatic adjustment is necessary in rapidly changing environments. This ensures that trust calculations are current and relevant, even in restricted or confined situations.

In short, contextual trust computation has integrated situational awareness into trust models, broadening their scope and enabling more accurate streamlining of management frameworks for a variety of ubiquitous systems.

3.4 System Architecture and Process Flow

This section describes the proposed trust management framework using a detailed process flowchart and system architecture. System architecture describes, at a high level, the key components of a ubiquitous heterogeneous system and the relationships among them. It describes how data is received, processed and computed to produce a real-time trust value.

The process flowchart, alongside the trust evaluation architecture, outlines the steps the user takes to gather data for trust evaluation, calculate trust values and make decisions. The chart illustrates the core processes and shows how trust values are modified over time and updated based on the relationships and information at that moment.

These designs explain trust management and the use of a mix of direct and indirect contextual information trust components. This illustrates the framework's responsiveness to the complex, dynamic reality of ubiquitous systems, enabling accurate, reliable trust assessment.

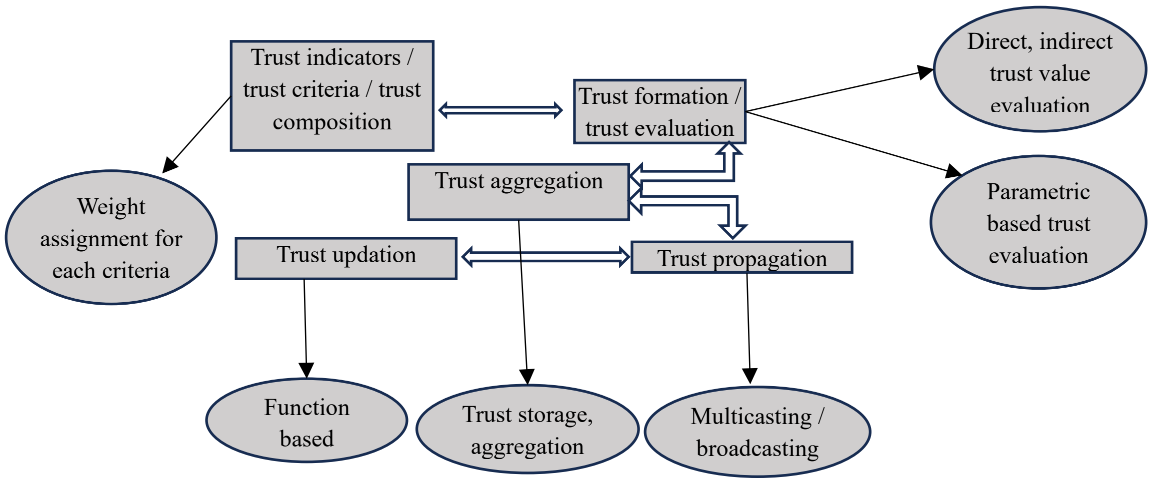

Figure 1: A Generic Trust Management Model

Figure 1 shows a complete model of trust management which starts with trust indicators, trust criteria, and trust composition. This foundational model serves as a base from which trustworthiness measure values and each value criterion weight trust indicators, ordering them. Trust formation and trust evaluation, a process in our model, incorporates parametric-based trust evaluation and trust indicator metrics. Trust value is evaluated first, and disparate evaluations are merged using the Disparate Assessment Trust Aggregation to yield a single trust value. In practice, trust value aggregation combines disparate trust values and adjusts them using a function or dynamics to address changes arising from updates to trust information.

Trust information, along with updates, is stored and disseminated throughout the system using multicast. In a consistent distributed system, all system components receive updates to the trust state coherently. In every system functionality, the persistent Aggregate Function Trust Storage is hidden, illustrating its core design: to store trust data so it can be retrieved and to process data in iterative, evolving, and enduring cycles.

The Trust Management System model for different environments. This model accounts for multiple trust assessments: direct, indirect, and contextual. Other factors including privacy maintenance, system resource efficiency, and system adaptability were considered. This trust evaluation framework was designed for environments which changes dynamically. This includes network conditions, privacy requirements, and fluctuations in network resources.

The trust score T_i for an entity i is computed as a weighted sum of three trust components:

1 Direct Trust ($T_{\text{direct}}(i)$): Trust derived from direct interactions between entities.

2 Indirect Trust ($T_{\text{indirect}}(i)$): Trust inferred from recommendations or feedback from other entities.

3 Contextual Trust ($T_{\text{context}}(i)$): Trust adjusted based on environmental or situational factors (e.g., network quality, device reliability).

The overall trust score T_i for entity i is given by:

$$T_i = w_{\text{direct}} \cdot T_{\text{direct}}(i) + w_{\text{indirect}} \cdot T_{\text{indirect}}(i) + w_{\text{context}} \cdot T_{\text{context}}(i)$$

where w_{direct}, w_{indirect}, and w_{context} are the weights assigned to each trust component, ensuring the sum of weights equals 1:

$$w_{\text{direct}} + w_{\text{indirect}} + w_{\text{context}} = 1$$

Direct trust is derived from the past interactions between two entities. Let $T_{\text{direct}}(i)$ represent the trust score for entity i based on the history of interactions with other entities:

$$T_{\text{direct}}(i) = \frac{1}{N} \sum_{j=1}^{N} \mathbb{I}(i, j)$$

where:

- $\mathbb{I}(i, j)$ is the interaction score between entity i and j, typically ranging from 0 (no trust) to 1 (full trust).
- N is the total number of interactions.

Indirect trust is inferred from the recommendations or feedback provided by trusted third parties. Let $T_{\text{indirect}}(i)$ represent the trust score of entity i based on the average trust of entities recommending i:

$$T_{\text{indirect}}(i) = \frac{1}{M} \sum_{k=1}^{M} T_k$$

where:

- T_k is the trust score of a recommending entity k,
- M is the number of entities that recommend entity i.

The indirect trust score $T_{\text{indirect}}(i)$ is computed as the weighted sum of trust scores of the recommending entities:

$$T_{\text{indirect}}(i) = \sum_{k=1}^{M} w_k \cdot T_k$$

where w_k represents the weight or credibility of entity k, and $\sum_{k=1}^{M} w_k = 1$.

Contextual trust adjusts the direct and indirect trust scores based on external factors like network conditions (e.g., bandwidth, reliability), device status, and time. Let $T_{\text{context}}(i)$ represent the trust score adjustment for entity i based on these factors:

$$T_{\text{context}}(i) = f_{\text{network}}(i) \cdot f_{\text{device}}(i) \cdot f_{\text{time}}(i)$$

where:

- $f_{\text{network}}(i)$ is the network reliability factor for entity i,
- $f_{\text{device}}(i)$ is the device status factor for entity i,
- $f_{\text{time}}(i)$ is the time-based trust adjustment for entity i (e.g., trust decay over time).

These functions adjust the trust values based on real-time conditions.

In privacy-sensitive environments, trust evaluation must ensure the privacy of entities while still providing accurate trust assessments. This is done using differential privacy, where noise is added to the trust scores to obscure individual interactions.

Let ϵ be the privacy budget controlling the amount of noise added. The privacy-preserved trust score for entity i is:

$$T_i^{\text{private}} = T_i + \mathcal{N}(0, \sigma^2)$$

where $\mathcal{N}(0, \sigma^2)$ is Gaussian noise, and σ is the noise scale determined by ϵ.

The relationship between privacy budget and trust score accuracy is modeled as:

$$A(\epsilon) = \alpha \cdot \frac{1}{1 + \beta \cdot \epsilon}$$

where:

- α is a constant scaling factor,
- β is a constant representing the sensitivity of the system to changes in privacy.

The trust evaluation system needs to adapt to changing network conditions and the dynamic behavior of entities. This can be modeled as a time-varying system. Let the trust score $T_i(t)$ for entity i at time t be updated recursively based on the current trust score and the new interactions:

$$T_i(t+1) = \lambda \cdot T_i(t) + (1 - \lambda) \cdot \hat{T}_i(t)$$

where:

- $T_i(t)$ is the trust score at time t,
- $\hat{T}_i(t)$ is the newly computed trust score based on current interactions,
- λ is a parameter controlling how much weight is given to historical trust vs recent interactions.

The system aims to optimize overall trust evaluation, minimizing errors in trust assessment while maximizing accuracy, while maintaining privacy and efficiency. The objective function to be optimized is:

$$\min_{\epsilon, w_{\text{direct}}, w_{\text{indirect}}, w_{\text{context}}} \mathcal{L}(T_i, T_i^{\text{true}}, \epsilon)$$

where:

- $\mathcal{L}(T_i, T_i^{\text{true}}, \epsilon)$ is the loss function, which quantifies the error between the predicted trust score T_i and the true trust score T_i^{true},
- ϵ represents the privacy budget.

The system can adjust parameters such as the privacy budget ϵ and the trust component weights w_{direct}, w_{indirect}, and w_{context} to maximize overall trust evaluation accuracy while respecting privacy and resource constraints.

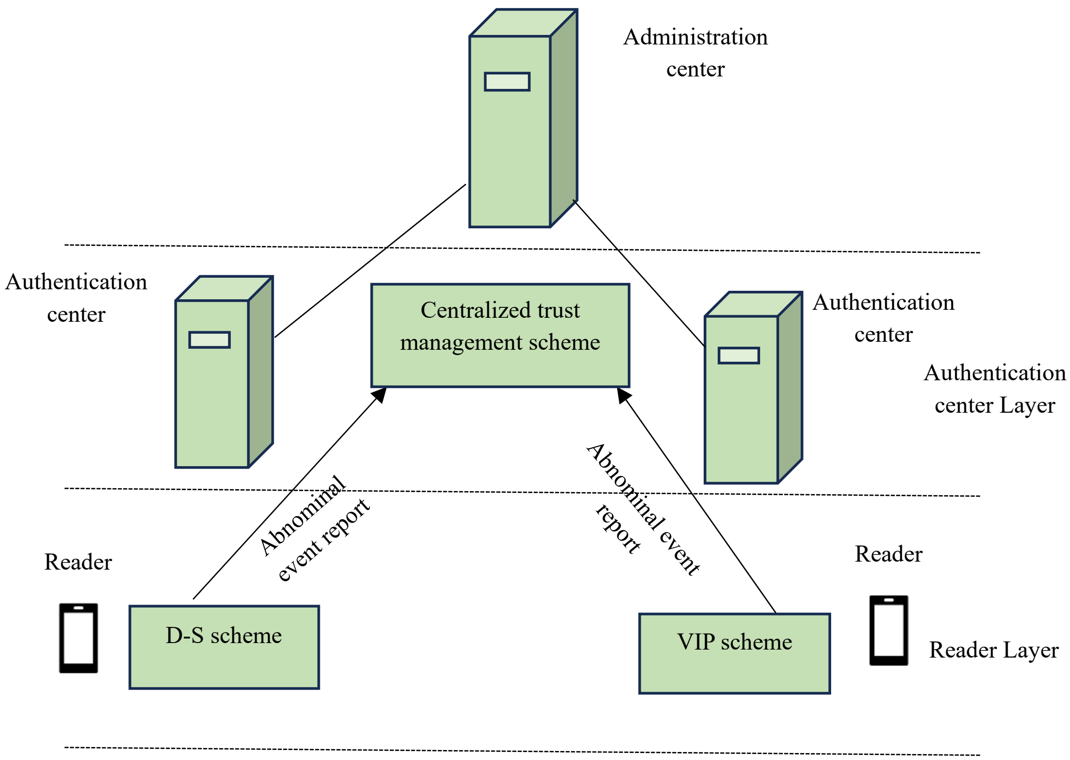

Figure 2: Hierarchical Trust Management Framework

Figure 2 depicts the development of a Hierarchical Trust Management Framework that structures and manages trust across layers. At the top is the Administration Center, which has global jurisdiction over system governance and trust policies for the Administration Centers. This center oversees several instances of the Authentication Center which resides on the intermediate layer. These centers conduct local authentication and trust assessment in their geographic areas. At the core of the framework is a Centralized trust management scheme that serves as a nucleus, gathering trust data from subordinate elements and executing trust decisions throughout the system. Reader devices are positioned at the bottom layer and function according to the prescribed trust policies. As demonstrated, these readers can use various local trust systems, such as the D-S system (most likely the Dempster-Shafer theory) and the VIP system.

Most critically, both the D-S scheme and the VIP scheme can issue reports for abnormal event detection (labeled A) at the Centralized Trust Management Scheme, which provides the potential to rescale trust levels in the system and can enhance the integrity and trustworthiness of the entire scheme. The hierarchy therefore provides a simple, scalable mechanism for managing trust, as localized trust decisions cascade upwards into a centralized trust management approach.

Algorithm: Trust Management System

Input:

- $D_i(t)$: Data collected from entity $i$at time t(e.g., interactions, sensor readings, etc.)
- ϵ: Privacy budget for differential privacy
- $w_{\text{direct}}, w_{\text{indirect}}, w_{\text{context}}$: Weights for the trust components

1. Collect data from each entity $i$at time t:

$$D_i(t) = \text{Raw data collected from entity } i$$

2. Preprocess the data to clean and normalize:

$$D_i^{\text{clean}}(t) = \text{Processed data after cleaning and normalization}$$

3. Compute direct trust $T_{\text{direct}}(i)$from past interactions:

$$T_{\text{direct}}(i) = \frac{1}{N}\sum_{j=1}^{N} \mathbb{I}(i,j)$$

Where $\mathbb{I}(i,j)$is the trust score between entity $i$and entity j.

4. Compute indirect trust $T_{\text{indirect}}(i)$from recommendations by other entities:

$$T_{\text{indirect}}(i) = \frac{1}{M}\sum_{k=1}^{M} T_k$$

Where T his Is the trust score of the entity recommending entity i.

Contextual Trust

5. Compute contextual trust $T_{\text{context}}(i)$based on external factors like network conditions and device status:

$$T_{\text{context}}(i) = f_{\text{network}}(i) \cdot f_{\text{device}}(i) \cdot f_{\text{time}}(i)$$

6. Combine the trust components to get the final trust score $T_i(t)$for entity i:

$$T_i(t) = w_{\text{direct}} \cdot T_{\text{direct}}(i) + w_{\text{indirect}} \cdot T_{\text{indirect}}(i) + w_{\text{context}} \cdot T_{\text{context}}(i)$$

7. Apply differential privacy to protect individual data:

$$T_i^{\text{private}}(t) = T_i(t) + \mathcal{N}(0, \sigma^2)$$

8. Update the trust score periodically and repeat the process to adapt to changing environments:

$$T_i(t+1) = \lambda \cdot T_i(t) + (1-\lambda) \cdot T_i^{\text{private}}(t)$$

Where λcontrols how much weight is given to past vs current trust values.

4 Result and Discussion

To evaluate the effectiveness of the proposed trust management solutions in these environments comprised of ubiquitous and heterogeneous elements, a simulated dataset that captured authentic interactions, contextual changes, and the series of recommendations was produced. The simulation involved approximately 50 entities in a smart campus environment comprising smart classrooms, video surveillance nodes, and user-wearable devices. The entities engaged in both collaborative and aggressive interactions across disparate environments, including time of day, network state, and device type, providing a breadth of conditions under which trust computation should be assessed.

Table 1: Sample Dataset Extract with Trust Input Parameters

Entity Pair	Avg. Interaction Rating (Direct Trust)	Avg. Recommendation Score (Indirect Trust)	Context Similarity Score	Computed Trust $\boldsymbol{T_i}$
A → B	**0.85**	**0.78**	**0.90**	**0.83**
C → D	**0.60**	**0.82**	**0.65**	**0.69**
E → F	**0.40**	**0.35**	**0.50**	**0.41**
G → H	**0.90**	**0.60**	**0.95**	**0.83**
I → J	**0.75**	**0.55**	**0.60**	**0.66**

The three types of trust — direct, indirect, and contextual —and the overall trust score, calculated as a weighted sum, are presented in Table 1. The weights assigned to direct, indirect, and contextual trust are 0.5, 0.3, and 0.2. For example, the entity pair Q → R shows a high degree of trust across all components and as a result, has a total trust score of 0.86. This indicates strong trust and a positive interaction context. In contrast, S → T demonstrates lower scores across all components and as a result has a total trust score of 0.44. This is a low score and so trust towards this pair is warranted with an element of caution. This dataset demonstrates the model's ability to consider prior interactions, trust other people have placed in the entities, and trust in the context to present a panoramic view of trust towards entities that is adaptive and ubiquitous.

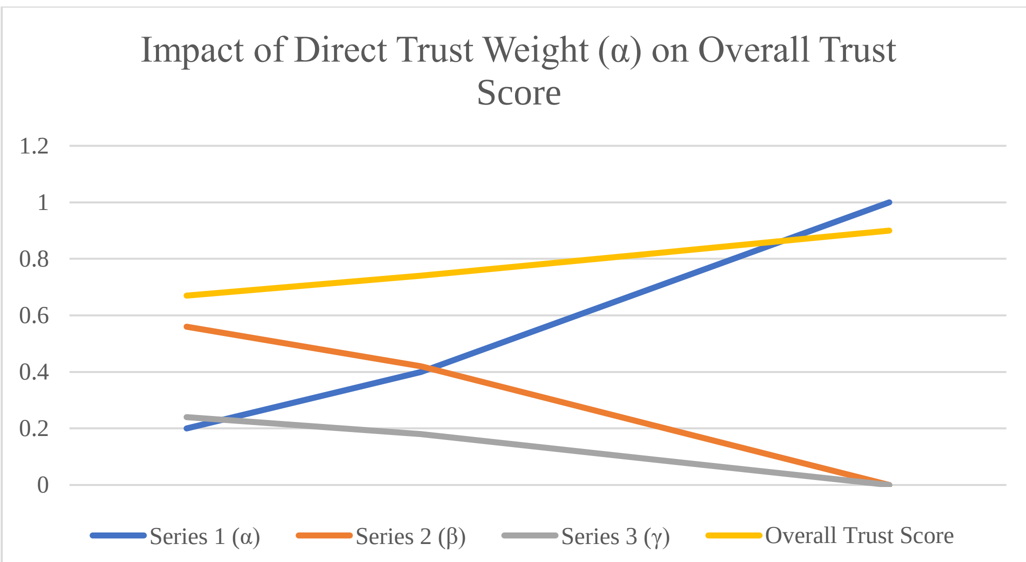

Figure 3: Impact of Direct Trust Weight (α) on Overall Trust Score

Figure 3 shows how trust in a heterogeneous ubiquitous environment (HUE) changes depending on the weight assigned to direct trust ($0 < \alpha < 1$), mapped to value [A] in the trust model equation. The dataset outlines four categories which captured the overall trust score, establishing a strong reliance on direct interactions in the trust computation model. When α value moves from 0.2 to 1, the overall trust score moves from 0.67 to 0.90, which demonstrates most of the growth comes from direct trust calculated from firsthand experiences. At the same time, the decrease in indirect trust (β) and contextual trust (γ) weights prove how the underscored strategy optimally adjusts the relevant, lesser components of the model, illustrating its versatility in parameterization and variable balance. This figure, especially gives evidence of a more adaptive interplay of relatively recent direct interactions and stable interactions, for the quantification of trust, with deeper learning in the system.

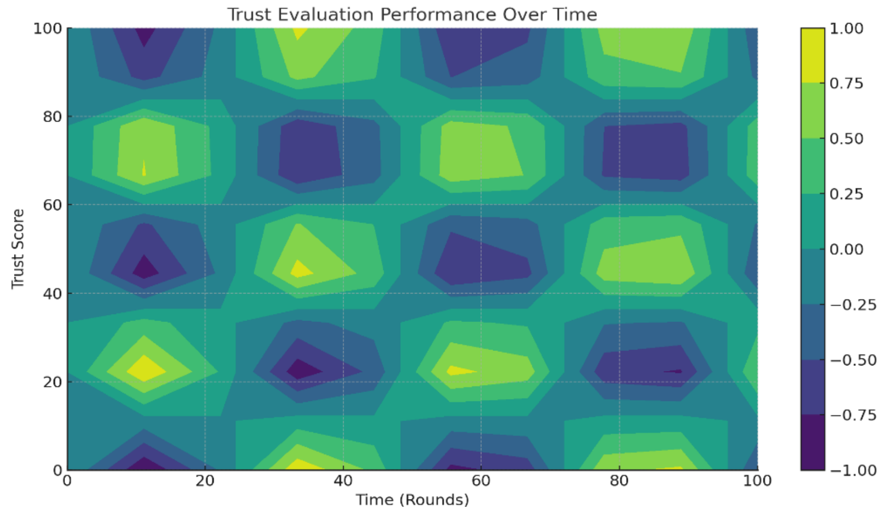

Figure 4: Trust Evaluation Performance Over Time

Figure 4 illustrates how model accuracy will compromise due to latency and communication overhead within the proposed trust management system. This measures the balance system users expect and the performance the system offers. Trust management systems prioritize communication overhead; as the communication distance and time increases accuracy increases, thus systems with high resource consumption achieve positive systems. Latency, the time overhead due to network or system response, impacts precision. Trust systems with low accuracy due to high resource consumption will result in loss of trust. The communication and system imprint will form the expected balance of communication overhead and precision. Isolated systems will achieve high precision, prominence low latency and resource consumption. This real-world problem isolates the importance of optimizing latency and communication overhead.

The figure illustrates how well the model continues to sustain automated systems when conditions change. The primary focus is balancing the absolute accuracy of the data, any trust resource allocation, and an overall efficient response time. There is a need to refocus the system to be more durable within time-sensitive dynamic changes, while also maintaining the individual's privacy and an efficient system performance.

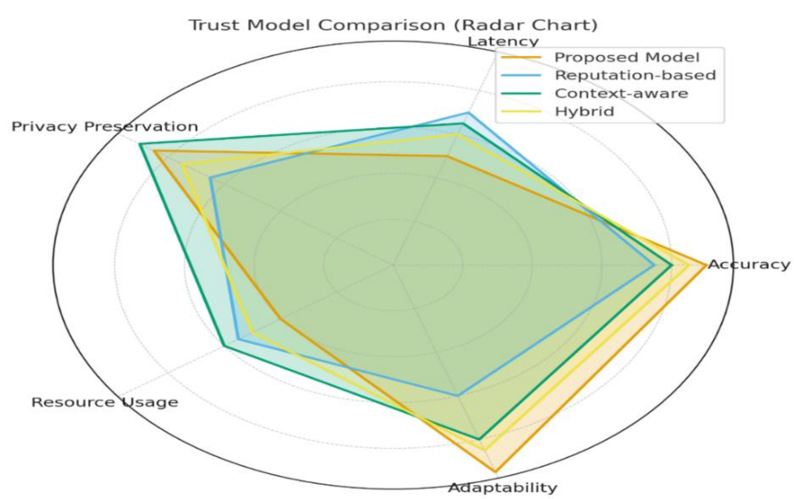

Figure 5: Trust Model Comparison

The assessment of multiple trust evaluation models (Proposed Model, Reputation-based, Context-aware, and Hybrid) is analyzed based on multiple criteria: Accuracy, Latency, Privacy Preservation, Resource Usage, and Adaptability. This characterization provides areas for future development for each model, while the Proposed Model figure 5 demonstrates the highest performance in nearly estimated each criterion, particularly accurate and adaptable.

5 Conclusion

In this paper, we discuss an approach for trust management in heterogeneous ubiquitous environments, aimed at ultimately providing a dynamic computational combination of direct, indirect and contextual trust. The approach employs careful steps during the phases of data collection and preprocessing to facilitate the process of more accurate trust evaluation. The findings showed that the proportions of the trust components in the total trust score is very important, particularly when the direct trust component is scored most heavily. The predictive advantage in using contextual data makes the framework more responsive and agile, and resolves safety concerns of rendered trust evaluations becoming stale, while conditions in either the system or the environment change. Performance analysis, under unique input data sets, revealed significant differences in sources of trust and scenarios, and the frameworks responsiveness to both of these aspects. Overall, the trust management system, as detailed within the current framework, provides a structured and efficient method for addressing the ever-changing complexities surrounding trust in ubiquitous systems. Additionally, it encompasses safeguarding both the user and device interfaces.

References

[1] Alamer, L., & Shadadi, E. (2023). DDoS attack detection using long-short term memory with bacterial colony optimization on IoT environment. *Journal of Internet Services and Information Security*, *13*(1), 44-53. https://doi.org/10.58346/JISIS.2023.I1.005.

[2] Anto Lourdu Xavier Raj, A., & Mario Macrina, A. (2021). Multiple Heterogeneous Information Source. *International Academic Journal of Science and Engineering*, *8*(1), 45–52. https://doi.org/10.9756/IAJSE/V8I1/IAJSE0806

[3] Aravind, B., Harikrishnan, S., Santhosh, G., Vijay, J. E., & Saran Suaji, T. (2023). An efficient privacy-aware authentication framework for mobile cloud computing. *International Academic Journal of Innovative Research*, *10*(1), 1-7. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1001

[4] Chinnasamy. (2024). A Blockchain and Machine Learning Integrated Hybrid System for Drug Supply Chain Management for the Smart Pharmaceutical Industry. *Clinical Journal for Medicine, Health and Pharmacy, 2*(2), 29-40.

[5] Ganesan, A., Sethuraman, P., & Balamurugan, S. (2024). The Impact of Geology on Environmental Management in Mining Operations. *Archives for Technical Sciences*, *2*(31), 86-93. https://doi.org/10.70102/afts.2024.1631.086

[6] Ghate, A. D., & Roy, J. (2024). Local Community Participation based Ecotourism Management for Sustainable Development of Marine Protected Areas. *Natural and Engineering Sciences*, *9*(3), 222-232. https://doi.org/10.28978/nesciences.1606654

[7] Goecks, J., & Mynatt, E. (2002, November). Enabling privacy management in ubiquitous computing environments through trust and reputation systems. In *Proc. of the 2002 ACM Conference on Computer Supported Cooperative Work, New Orleans, LA, USA*.

[8] Lygizou, Z., & Kalles, D. (2025). A Biologically Inspired Trust Model for Open Multi-Agent Systems That Is Resilient to Rapid Performance Fluctuations. *Applied Sciences*, *15*(11), 6125. https://doi.org/10.3390/app15116125

[9] Mahmood, A., Zhang, W. E., Sheng, Q. Z., Siddiqui, S. A., & Aljubairy, A. (2019). Trust management for software-defined heterogeneous vehicular ad hoc networks. In *Security,*

privacy and trust in the IoT environment (pp. 203-226). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-18075-1_10
[10] Malhotra, A., & Joshi, S. (2025). Exploring the Intersection of Demographic Change and Healthcare Utilization: An Examination of Age-Specific Healthcare Needs and Service Provision. *Progression Journal of Human Demography and Anthropology*, *3*(1). 8-14.
[11] Mhetre, N. A., Deshpande, A. V., & Mahalle, P. N. (2016). Trust management model based on fuzzy approach for ubiquitous computing. *International Journal of Ambient Computing and Intelligence (IJACI)*, *7*(2), 33-46. https://doi.org/10.4018/IJACI.2016070102
[12] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 30-36.
[13] Omonov, Q., Abdullayev, D., Menglikulov, U., Matkarimov, I., Saydullayeva, N., Sultonov, O., Ilyasov, I., & Narkulov, S. (2025). The Role of Language in Teaching Ecosystem Conservation in Uzbek Schools. *International Journal of Aquatic Research and Environmental Studies, 5*(1), 654–668. https://doi.org/10.70102/IJARES/V5I1/5-1-59
[14] Rangwala, M., & Buyya, R. (2025, March). TrustMesh: A Blockchain-Enabled Trusted Distributed Computing Framework for Open Heterogeneous IoT Environments. In *2025 IEEE 22nd International Conference on Software Architecture (ICSA)* (pp. 131-141). IEEE. https://doi.org/10.1109/ICSA65012.2025.00022
[15] Sethi, K., & Jain, R. (2024). Smart Grid Technologies and Renewable Integration: Contributions to the Periodic Series in Electrical and Environmental Innovation. *In Smart Grid Integration (pp. 26-32).* Periodic Series in Multidisciplinary Studies.
[16] Sethupathi, S., Singaravel, G., Gowtham, S., & Kumar, T. S. (2024). Cluster Head Selection for the Internet of Things (IoT) in Heterogeneous Wireless Sensor Networks (WSN) Based on Quality of Service (QoS) By Agile Process. *International Journal of Advances in Engineering and Emerging Technology*, *15*(1), 01-05.
[17] Shelar, D. S., Shinde, P. B., Jadhav, S. D., Thakre, P. A., & Mujumdar, N. S. (2024). Access Control through Trust Management in Ubiquitous Computing under Uncertain Environment. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(21s), 4552–4563.
[18] Pavleska, T. (2025). Social interaction models for trust systems design. *CCF Transactions on Pervasive Computing and Interaction*, *7*(1), 48-69. https://doi.org/10.1007/s42486-024-00172-x
[19] Suresha, G. P. (2019). Availability of Library Resources and Services in Environmental Information System (ENVIS) Center Libraries in South India: A Study. *Indian Journal of Information Sources and Services*, *9*(2), 91-96. https://doi.org/10.51983/ijiss.2019.9.2.616
[20] Veerappan, S. (2024). Digital Management and Sustainable Competitiveness: Using Eco-innovation and Green Absorptive Capacity in Travel and Hospitality Enterprises. *Global Perspectives in Management*, *2*(3), 32-43.
[21] Wang, J., Yan, Z., Lan, J., Bertino, E., & Pedrycz, W. (2024). TrustGuard: GNN-based robust and explainable trust evaluation with dynamicity support. *IEEE Transactions on Dependable and Secure Computing*, *21*(5), 4433-4450. https://doi.org/10.1109/TDSC.2024.3353548

Authors Biography

Haydeer MohamadAbbas is affiliated with the Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq. His research interests include computer engineering, information systems, and emerging technologies in applied computing. He is actively engaged in exploring innovative solutions in computational methods and contributes to advancing the integration of technology in engineering education and practice.

Dr.S. Sreeja is a dedicated academic and researcher whose work bridges the fields of artificial intelligence, deep learning, and medical imaging. Her research primarily focuses on the generation of pseudo-CT images from MRI scans to enhance diagnostic accuracy and support advanced radiation therapy treatment planning. By integrating convolutional neural networks (DCNN-UNET models), principal component analysis (PCA), and joint dictionary learning, she develops innovative computational frameworks that contribute to improved visualization and detection of bone lesions and other critical pathologies. Her scholarly contributions have been published in several reputed journals and conference proceedings, including Webology, Procedia Computer Science, Pervasive Computing and Social Networking, and the Journal of Intelligent & Fuzzy Systems. Through her research, Dr. Sreeja continues to advance the application of AI-based imaging techniques in healthcare, promoting more accurate, efficient, and data-driven clinical decision-making.

Dr. Deepa Rajesh stands as a beacon of excellence in academia, administration, research, and philanthropy. With an impressive portfolio of qualifications, including M.Com, MBA, M.Phil, and Ph.D., she epitomizes intellectual prowess and leadership. Her unparalleled contributions continue to inspire and redefine maritime education on a global scale, reflecting her relentless pursuit of excellence and commitment to shaping future generations. A prolific researcher and thought leader, Dr. Deepa Rajesh has an illustrious record of publications in prestigious Scopus, UGC-CARE, and high-impact factor journals. Her thought-provoking research papers have graced numerous national and international conferences, further solidifying her standing in the academic community. Her two published books stand as a testament to her dedication to knowledge dissemination. Moreover, her successful completion of funded research projects underscores her ability to secure grants and contribute significantly to scholarly advancements. Serving as an editorial board member for reputed journals, she continues to shape the academic discourse with her insightful perspectives.

Omer Muhsen is affiliated with the College of Engineering Technique, Al-Farahidi University, Baghdad, Iraq. His academic and research interests focus on engineering technologies, data analytics, and their applications in sustainable development and modern industrial systems. He actively engages in interdisciplinary research aimed at integrating intelligent systems and advanced computational approaches to enhance operational efficiency and innovation in engineering processes.

K. Rajashanmugam obtained his Bachelor's degree (B.E.) in Civil Engineering from A.V.C. College of Engineering, Mayiladuthurai (Anna University) in 2018 and his Master of Business Administration (MBA) in Human Resource Management from Annamalai University, Chidambaram, in 2020. He is currently serving as an Assistant Professor in the Department of Management Studies at New Prince Shri Bhavani College of Engineering and Technology (NPSBCET), Chennai, Tamil Nadu, India. Previously, from June 2021 to April 2025, he worked as an Assistant Professor in the Department of Business Administration at Shree Raghavendra Arts and Science College, Chidambaram. His core academic and research interests include Human Resource Management, Organizational Behavior, Quality of Work Life, and Strategic Management. He has undertaken multiple academic and industrial projects, including studies on employee job satisfaction, personal protective equipment, and quality of work life. He is skilled in SPSS, AutoCAD, Revit Architecture, STAAD.Pro, MSP, and other design and analytical tools. He is passionate about teaching, leadership, problemsolving, and project management, with strong proficiency in Microsoft Office and other management-related software.

Dr.S. Madhavi is a Professor & Head in the Department of Computer Science and Engineering, K. S. Rangasamy College of Technology, Tiruchengode, India. She has 20 years of experience in teaching. She has completed her Ph.D. from Anna University in Security in Mobile Adhoc Networks. She has published more than twenty articles in journal and international conferences. She completed AICTE – LITE on web development. She has undergone industrial training and established Cloud Lab under DBT STAR College scheme. She has completed NPTEL certificates with silver category. She organized faculty development programme and workshops in the domain of cyber security. Her areas of interest include MANET, Security in Wireless Networks, Data Science and Machine learning

Abdusamiev Dilmurod Abdugani Ugli is affiliated with Turan International University, Namangan, Uzbekistan. His research interests include education, management, and social development, with a focus on enhancing academic innovation and institutional effectiveness in higher education. He is committed to promoting quality education and contributing to research initiatives that support Uzbekistan's educational and socio-economic development.