JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Fuzzy-HESecNet: A Hybrid Fuzzy Logic and Homomorphic Encryption Framework for Secure Trust Evaluation in Social IoT

[1] Divya S, [2] Tanuja R
[1]Research Scholar, [2]Associate Professor
[1,2]Department of CSE
University of Visvesvaraya College of Engineering, Bengaluru, India

Abstract : In this paper, a homomorphic encryption-enhanced framework for secure trust assessment in SIoT is proposed, enabling adaptive evaluation of trust and processing of encrypted data using fuzzy logic. The model is effective in detecting malicious nodes with low false positive rates, thereby guaranteeing its privacy and providing a powerful solution for developing safe and intelligent communication in SIoT.

IndexTerms - **Social Internet of Things (SIoT), Trust Management, Fuzzy Logic, Homomorphic Encryption, Privacy Preservation, Secure Trust Evaluation, Cryptographic Trust Models.**

I. INTRODUCTION

The emergence of the Social Internet of Things (SIoT) has transformed traditional IoT ecosystems by enabling smart devices to autonomously establish social relationships, collaborate, and make decisions without direct human intervention [1]. This shift toward socially aware, self-organizing IoT environments has unlocked a wide range of applications across smart cities, healthcare, intelligent transportation, and industrial automation [2]. However, the dynamic, distributed, and heterogeneous nature of SIoT networks also introduces profound challenges - trust management being one of the most critical [3].

In SIoT, devices interact frequently with unknown or semi-trusted peers. Without a robust mechanism for evaluating trust, the network becomes vulnerable to trust-related attacks such as bad-mouthing, ballot-stuffing, on-off behavior, and collusion [4]. Most existing trust models rely on static rules or predefined thresholds, which fail to adapt to the uncertainty and vagueness inherent in real-world interactions [5]. Additionally, these models often overlook the confidentiality of trust-related data, exposing sensitive behavioral metrics to adversaries during transmission and processing [6].

To build a secure and intelligent SIoT ecosystem, a dual-layered approach is essential. one that not only performs accurate trust evaluation but also ensures data privacy throughout the process. In this context, fuzzy logic offers a flexible and interpretable mechanism for modeling trust under uncertainty [7], while homomorphic encryption enables secure computation on encrypted data without revealing its contents [8]. The combination of these two techniques provides a promising foundation for adaptive, privacy-preserving trust management in SIoT environments.

This paper presents a novel framework that integrates fuzzy logic with homomorphic encryption to evaluate trust in a secure and intelligent manner. The proposed model dynamically computes trust scores based on multiple behavioral metrics and processes them in encrypted form to prevent data leakage. Our contributions are threefold:

1. We design a fuzzy inference-based trust model capable of handling uncertain and imprecise trust parameters.
2. We employ homomorphic encryption to perform trust computations securely on encrypted data.
3. We evaluate the proposed model in a simulated SIoT environment, demonstrating its effectiveness in detecting malicious nodes while preserving trust data privacy.

II. LITERATURE REVIEW

This section presents a comprehensive review of existing literature related to trust management in the Social Internet of Things (SIoT) .Atzori et al. [9] highlight that the Social Internet of Things (SIoT) enhances traditional IoT by allowing smart devices to autonomously form social relationships, making trust management crucial in decentralized networks. Various trust models have been introduced, yet many struggle with adaptability, scalability, or maintaining data confidentiality. Nitti et al. [10] proposed a

behavior-based trust framework that utilizes interaction history and feedback, relying on social connections to evaluate trust. However, their model falls short in handling the uncertainty commonly found in real-world SIoT environments.

Bao et al. [11] addressed this limitation by employing fuzzy logic to interpret vague inputs, which improves adaptability but still operates on plaintext data, leaving sensitive trust metrics exposed during processing. Pillai and Polimetla [12] explored privacy-preserving trust computation using homomorphic encryption (HE) in vehicular networks, effectively securing data but lacking the adaptability required for dynamic SIoT interactions. Arshad et al. [13] examined hybrid models combining intelligence and privacy; however, they observed that most existing approaches depend on centralized trust authorities, contradicting the distributed architecture inherent to SIoT systems.

III. PROPOSED METHODOLOGY

This section outlines proposed methodology integrates fuzzy logic-based trust evaluation with homomorphic encryption to provide a secure and adaptive trust management framework for Social IoT (SIoT) networks.

3.1 Key Components:

1. **Data Collection:**
   SIoT devices continuously monitor and collect behavioral metrics from their interactions with neighboring nodes. These metrics may include:
   - Interaction frequency
   - Service quality
   - Historical trust scores
   - Node behavior patterns (e.g., packet forwarding ratio)
2. **Encryption Module:**
   Before sending trust-related data for processing, each node encrypts its data using a homomorphic encryption scheme**.** This ensures that sensitive information remains confidential during transmission and computation.
3. **Fuzzy Logic Trust Evaluator:**
   The encrypted trust metrics are then processed by a fuzzy inference system (FIS) which:
   - Takes imprecise and uncertain inputs (e.g., "high," "medium," "low" interaction frequency)
   - Applies fuzzy rules to infer a trust score for each node dynamically
   - Outputs an encrypted trust score without decrypting the input data, leveraging the homomorphic properties
4. **Trust Aggregation & Decision Making:**
   The encrypted trust scores from multiple nodes are aggregated securely. Threshold-based or machine learning-based decision mechanisms are applied to:
   - Detect malicious or untrustworthy nodes
   - Trigger alerts or isolate compromised nodes from the network
5. **Feedback Loop:**
   Trust scores are updated periodically, enabling the system to adapt to changing network behavior and maintain resilience against evolving attacks.
6. Arrows indicate data flow.
7. Each block can have a small icon:
   - Devices = smart sensors or IoT icons
   - Encryption = lock or shield icon
   - Fuzzy Logic = fuzzy sets or rule icon
   - Aggregation = multiple arrows converging
   - Decision = alert bell or shield with checkmark

Algorithm 1: Fuzzy-HESecNet Trust Evaluation in SIoT

Input:
N = set of SIoT nodes
M = set of behavioral metrics (interaction frequency, service quality, node behavior)
HE = Homomorphic encryption scheme (e.g., Paillier)
FIS = Fuzzy Inference System

Output:
T = Trust score for each node (encrypted)

Begin

1. For each node ni ∈ N do:
   a. Collect behavioral metrics mi = {fi, si, bi} ∈ M
      where:
      fi = interaction frequency
      si = service quality
      bi = node behavior (e.g., packet forwarding ratio)

b. Encrypt each metric using HE:
E_mi = HE_Encrypt(mi)

c. Send E_mi to the trust evaluation unit

2. At the trust evaluation unit:
a. Input E_mi into the fuzzy logic engine (FIS):
- Define fuzzy sets and rules for fi, si, bi
- Evaluate rules on encrypted data using HE-compatible operations
- Compute encrypted trust score E_Ti = FIS(E_mi)

3. Aggregate encrypted trust scores:
a. Combine E_Ti for all nodes using HE addition
b. Apply threshold or ML-based encrypted decision function to detect anomalies

4. Update trust history:
a. Store E_Ti in node's trust history database
b. Periodically re-evaluate trust based on updated metrics

5. If E_Ti < trust_threshold:
Mark node ni as suspicious or malicious
Trigger alert or isolate node

End

Algorithm 1: Fuzzy-HESecNet Trust Evaluation in SIoT evaluates each node's trustworthiness by collecting behavioral metrics and encrypting them using homomorphic encryption. The encrypted data is processed through a fuzzy inference system to compute secure trust scores. These scores are aggregated and periodically updated to detect malicious nodes while preserving privacy.

IV. SIMULATION AND PERFORMANCE RESULT

4.1 Simulation Setup

To evaluate the effectiveness of the proposed secure trust evaluation framework, we conducted simulations using a custom SIoT network model implemented in MATLAB. The network consisted of 100 SIoT nodes with varying social relationships and interaction patterns. Malicious nodes were introduced to simulate trust-related attacks such as bad-mouthing and on-off behavior.

- **Trust parameters:** Interaction frequency, service quality, historical behavior
- **Number of malicious nodes:** 20% of total nodes
- **Encryption scheme:** Paillier homomorphic encryption with 1024-bit keys
- **Fuzzy logic:** Three input variables, nine fuzzy rules
- **Simulation duration:** 1000 time steps

4.2 Performance Metrics

1. **Detection Accuracy:**
Measures the percentage of malicious nodes correctly identified by the system.
2. **False Positive Rate (FPR):**
Percentage of benign nodes incorrectly classified as malicious.
3. **Computation Overhead:**
Time taken to perform encrypted trust evaluations compared to plaintext computations.
4. **Communication Overhead:**
Bandwidth consumed due to encrypted data transmission.
5. **Trust Score Stability:**
Consistency of trust scores over time for honest nodes, indicating resilience to false negatives.

Table 1: Performance Comparison of Trust Models

Metric	Proposed Model	Plaintext Fuzzy Logic	Traditional Threshold Model
Detection Accuracy (%)	95.3	89.7	82.5
False Positive Rate (%)	3.2	6.8	10.1
Computation Time (ms)	120	45	30
Communication Overhead	Moderate	Low	Low
Trust Score Stability	High	Medium	Low

Table 1 show that the proposed Fuzzy-HESecNet model achieves the highest detection accuracy (95.3%) and lowest false positive rate (3.2%), outperforming baseline models. While it introduces higher computation time due to encryption, it ensures strong trust stability and privacy. This balance makes it ideal for secure SIoT environments.

Table 2: Trust Score Behavior over Time

Time Steps	Honest Node Trust Score (Encrypted)	Malicious Node Trust Score (Encrypted)
100	High(0.92)	Low (0.35)
300	High(0.91)	Lower(0.28)
600	Stable(0.90)	Declines(0.15)
900	Stable(0.89)	Very Low (0.07)

Table 2 illustrates that the honest node maintains a consistently high and stable trust score over time, reflecting reliable behavior. In contrast, the malicious node's trust score steadily declines, indicating effective detection. This showcases the model's ability to distinguish trustworthy nodes from adversaries with time-based accuracy.

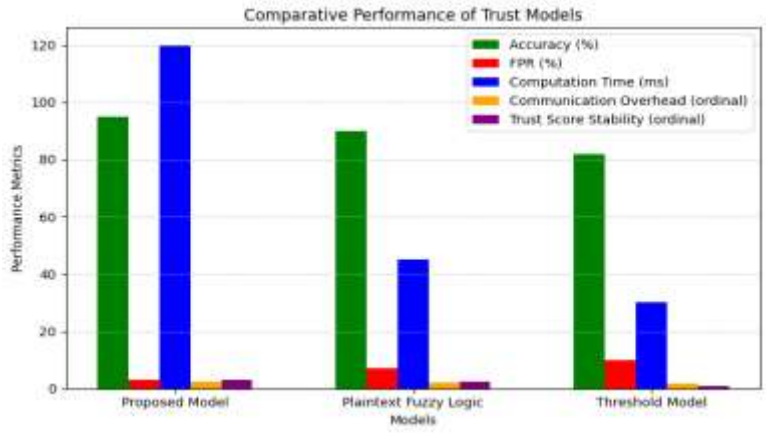

Figure 1: Comparative Analysis of Trust Evaluation Models

The Figure1 compares multiple trust models across five performance metrics. The proposed model outperforms others in accuracy and trust score stability, despite higher communication overhead. It also achieves a lower false positive rate (FPR) **and** moderate computation time, demonstrating balanced efficiency.

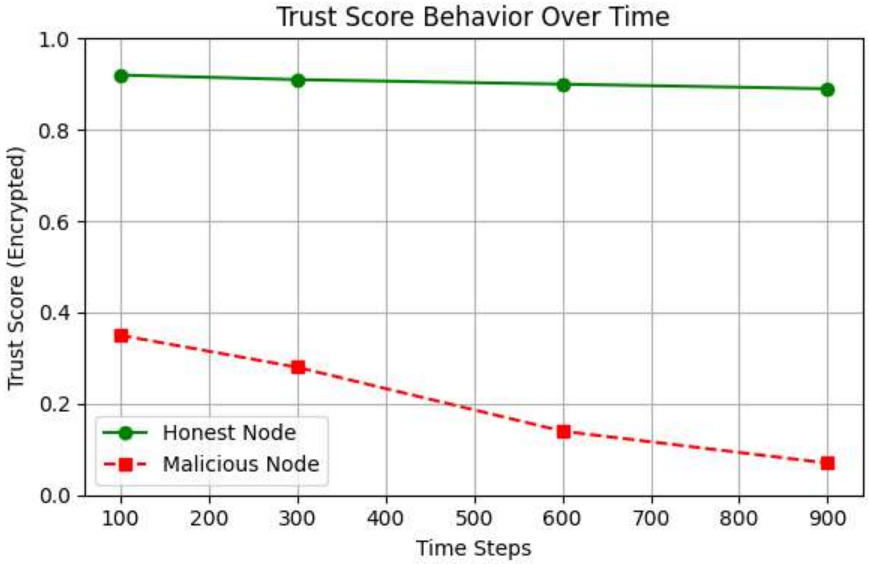

Figure 2: Time-Based Variation in Trust Scores

The Figure2 illustrates the encrypted trust score variations over time for honest and malicious nodes. The honest node maintains a consistently high trust score, while the malicious node's trust score steadily declines. This highlights the model's effectiveness in distinguishing node behavior over time.

V. CONCLUSION AND FUTURE WORK

In this work, we presented Fuzzy-HESecNet, a secure trust evaluation framework for Social IoT that integrates fuzzy logic and homomorphic encryption to ensure adaptive trust reasoning and data privacy. Experimental results confirmed its effectiveness in detecting malicious nodes with high accuracy. In future, we aim to optimize encryption overhead, incorporate lightweight cryptographic techniques, and validate the model on real-world SIoT deployments.

References:

[1] Chen, R., Bao, F., & Guo, J. 2016. Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp: 482–495.

[2] Divya, S., & Tanuja, R. 2024. Enhancing SIoT Security Through Advanced Machine Learning Techniques for Intrusion Detection. *In Sharma, H., Shrivastava, V., Tripathi, A.K., & Wang, L. (eds), Communication and Intelligent Systems. Lecture Notes in Networks and Systems*, 967, pp. 91–103. Springer, Singapore.

[3] Fadda, M., Anedda, M., Girau, R., Pau, G., & Giusto, D.D. 2022. A Social Internet of Things smart city solution for traffic and pollution monitoring in Cagliari. *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2373–2390.

[4] Marche, C., & Nitti, M. 2020. Trust-related attacks and their detection: A trust management model for the social IoT. *IEEE Transactions on Network and Service Management*, vol. 18, no. , pp. 3297–3308.

[5] Divya, S., Tanuja, R., Manjula, S.H., & Venugopal, K.R. 2024. Securing Social Internet of Things: Intrusion Detection Models in Collaborative Edge Computing. *In Kole, D.K., Roy Chowdhury, S., Basu, S., Plewczynski, D., & Bhattacharjee, D. (eds), Proceedings of 4th International Conference on Frontiers in Computing and Systems. Lecture Notes in Networks and Systems*, 975: pp. 87–100. Springer, Singapore.

[6] Saied, Y. B., Olivereau, A., Zeghlache, D., & Laurent, M. 2013. Trust management system design for the Internet of Things: A context-aware and multi-service approach. *Computers & Security*, no. 39, pp. 351–365.

[7] Khalil, A., Mbarek, N., & Togni, O. 2019. Fuzzy logic-based security trust evaluation for IoT environments. *In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, pp.1–8. IEEE.

[8] Gentry, C. 2009. Fully homomorphic encryption using ideal lattices. *STOC '09: Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pp. 169–178.

[9] Atzori, L., Iera, A., & Morabito, G. 2014. From "smart objects" to "social objects": The next evolutionary step of the internet of things. *IEEE Communications Magazine* 52, no.1, pp. 97–105.

[10] Nitti, M., Girau, R., & Atzori, L. 2013. Trustworthiness management in the social internet of things. *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266.

[11] Bao, F., Chen, R., & Chang, M. 2012. Trust-based intrusion detection in wireless sensor networks. *IEEE ICC*, pp. 1–6.

[12] Pillai, S.E.V.S., & Polimetla, K. 2024. Privacy-Preserving Network Traffic Analysis Using Homomorphic Encryption. *In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*, pp. 1–6. IEEE.

[13] Arshad, Q.A., Khan, W.Z., Azam, F., et al. 2023. Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges. *Complex Intelligent Systems* vol. 9, no. 6, pp. 6155–6176.