Findings

Name of the scholar: Himani Tyagi **Notification No. 589/2025**

Name of the Supervisor: Prof Rajendra Kumar **Date of Notification:25-11-2025**

Name of the Department: Department of Computer Science

Title: Development of Trust Management System for IoT

The Internet of Things is a modern technology that is directed at easing human life by automating most of the things used in daily life. The never-ending dependency on the network for communication is attracting adversaries to exploit the vulnerabilities of IoT. Therefore, this technology is facing some serious issues and challenges concerning security and privacy. The main vulnerabilities are different types of internal and external attacks that are addressed in this research.

The commonly available security solutions for IoT include Intrusion Detection Systems (IDS) and Trust Management Systems (TMS). IDS are security systems that identifies anomaly and attacks in IoT environment whereas TMS are security management system that evaluates and manages the trust between nodes such that nodes with malicious intent can be avoided and alarms can be generated. These systems promote node cooperation, manages energy of nodes, improve network lifetime, and prevent attacks. Therefore, this study proposes a Trust Management System for IoT networks using deep learning. Therefore, an extensive survey on TMS is presented in **contribution one** that includes a detailed discussion about security and privacy challenges, as well as available solutions for IoT based wireless sensor networks. The survey includes a systematic literature review (SLR) on Trust Management System (TMS) in IoT. With this, trust management schemes are classified into four groups based on the methodology used for implementing trust-based security solutions in the IoT: cryptography-based, computational and probabilistic-based, information theory-based, and Machine or Deep Learning based. It also enables the identification of gaps and limitations in the existing systems that need immediate attention. It also aims to identify the required characteristics of a Trust Management System (TMS) for IoT.

After a detailed Literature review, we have observed that two types of attacks are common in IoT networks: routing-based/internal attacks and non- routing-based attacks/external attacks. Additionally, our findings suggest that Deep Learning based approaches are effective in dealing with existing gaps and limitations.

Therefore, in the **second contribution,** we have proposed a TMS for two types of non routing based attacks/external attacks-DDoS and DoS. Fuzzy logic based trust evaluation model using Direct behavioural patterns, like network flows is proposed. The proposed system uses trapezoidal membership function model the behaviours sets in scale of 0 and 1.0 showing less trustworthy membership and 1 highest trustworthy membership to the set. The proposed model shows high 97% accuracy in clustering trustworthy and untrustworthy nodes. With this contribution, it is clear that only direct observable features are not enough for dealing with internal attacks, and hence, the third contribution contributes to searching for common and serious routing attacks prevalent in IoT.

However, the existing systems for internal attacks possess specific gaps like lack of real time trustworthiness evaluation and prediction system, unavailability of correct trust indicators, and unavailability of RPL specific dataset. Furthermore, it is proposed that current systems are inadequate for addressing the complexities of big data processing, inefficient to address all four common types of internal attacks, and isolating untrustworthy nodes to avoid further communication.

In **fourth contribution** a real time trust evaluation model is proposed against blackhole attack. Blackhole attacks is one type of internal attacks. The attacks try to capture all the packets by fooling the legitimate node and showing itself to be the best path and later discarding all the packets. Therefore, the multicriteria decision making problem is converted into single criteria time series based decision making problem using an Artificial intelligence based Principal Component Analysis (PCA) algorithm. When evaluating a node's trust value three parameters—direct, indirect and data- are considered. Then, three types of models are trained on the nodes behaviors, and the predicted values are recorded. Then a comparison between these three types of models namely traditional (AR, ARIMA) machine (RF, DT, XGBoost, AdaBoost), and deep learning approaches (LSTM, BI-LSTM), is performed. The proposed deep learning model (Bi-LSTM) can accurately and efficiently predict the nodes trustworthiness and restrict further communication with less trustworthy nodes. Thereby protecting the network from malicious nodes and increasing the network lifeline. The proposed demonstrated consistent performance with varying data sizes. For instance, with 25% of the dataset (over 0.1 million samples), the model achieved MSE of 0.008, RMSE of 0.089, MAE of 0.043, and an R^2 of 0.943. With 100% of the dataset (over 0.44 million samples), the results were even more impressive, with MSE of 0.005, RMSE of 0.07, MAE of 0.0256, and R^2 of 0.943, whereas Machine learning shows best performance as MSE of 0.008(for 50% data size),

RMSE of 0.089(for 50% data size), MAE of 0.034(for 50% data size) and 0.941 R^2 (for 25% data size) and traditional approach drastically fail to solve time series based big data problem. Hence, the model is also effective in addressing this Big Data problem.

Further, In fifth contribution, a set of trust indicators as proposed in previous contributions -Direct Trust (based on behaviours), Indirect Trust (based on rewards and punishments), and Data Trust (based on deviations in sensor values) show promising results in analyzing and predicting a nodes behavior in real time. The set is represented with a single value using the beta distribution function, which incorporates a balanced set of good and bad behaviours. This approach addresses the subjectivity often introduced by traditional weighted summation methods used in literature. Additionally, Kernal based Extreme Learning Machine is employed in this research. It is an advanced paradigm that uses various kernel functions to quickly solve non-linear problems. It also has good generalizability and works well on unseen and uncertain conditions. In this study we have showed the capabilities of KELM on unseen and non linear data. The proposed TMS is validated against four types of trust-based attacks—Blackhole, Decreased Rank, Version Number, and Flooding—which have not been adequately addressed in existing literature. The performance of proposed model is also validated on binary and multiclassification. Comparisons existing linear and non-linear machine learning models demonstrate that the proposed system outperforms current state-of-the-art TMS solutions, achieving 99.95% accuracy, 99.9% precision, 99.96% recall, and a minimal misclassification rate of just 0.05%.. The proposed model converges fast and accurately for trust prediction in IoT.

Further**, in sixth contribution** a lightweight, robust, scalable, and efficient trust-based security system TOMLDIoMT tailored for IoMT environments using KELM is proposed. IoMT is a subfield of IoT, which includes various medical monitoring device, gateways, cloud servers, and applications. Additionally, using the same set of trust indicators, all four types of routing attacks are detected and mitigated with high accuracy and low false alarms. Further, the performance of a machine learning model rely on hyper parameters. Hence, the proposed TMS using an automatic optimizer: optuna is proposed. The work clearly shows the capability of this framework for quickly searching correct parameters for training the model. The proposed TMS is validated on two datasets and against six types of internal attacks like Blackhole, Decreased Rank, Version Number, Flooding, spoofing and data manipulation, which have not been adequately addressed in existing literature. Furthermore, a stacked model is also proposed

due to the inability of a single model to detect all four types of attack. The performance of proposed machine learning based model is validated on two benchmark datasets, IoMT based WUSTL2020 and ROUT-4-2023. The limitations in the datasets like class imbalance and missing values are addressed through the Synthetic Minority Over-Sampling Technique (SMOTE) and preprocessing respectively. Various Machine Learning models like ELM (Extreme Learning Machine), XGBoost (Extreme gradient Boosting), RF (Random Forest), KNN (K Nearest Neighbour), SGB (Stochastic gradient boosting) and LR (Logistic Regressor) are trained. The effectiveness of these models heavily depends on their hyperparameters. Manually tuning them is time-consuming and often fails to yield optimal results. Therefore, in this research we have discussed the functionality of automatic optimization framework OPTUNA. The best results are shown by Random Forest (RF) achieving accuracies between 99.93% and 99.7% and a FAR of 0 to 0.1%. The experimental results demonstrate that the proposed framework outperforms existing state-of-the-art solutions.

In conclusion, the proposed framework exhibits strong capabilities for timely, accurate, and efficient trust assessment and prediction in IoT environments. The performance of the Trust Management System (TMS) is enhanced by introducing a novel set of trust indicators—Direct, Indirect, and Data trust. Additionally, four techniques were examined for trust aggregation process: fuzzy logic, beta distribution, and Principal Component Analysis (PCA). Experimental findings revealed that the fuzzy logic-based approach achieved the lowest accuracy, while the beta distribution and PCA-based methods delivered the highest accuracy. The results further demonstrate that the deep learning–enabled TMS significantly improves RPL-based IoT network performance in terms of accuracy, efficiency, and timely attack detection. Further, the capability of a lightweight version of Neural Network Kernal based Extreme Learning Machine (KELM) are also explored. The experimental results illustrate the potential of KELM for trust prediction in IoT. Moreover, the proposed TMS is highly effective in mitigating a range of routing attacks, including blackhole, flooding, rank, and version number. Comparative analysis against existing trust management systems highlights its superior performance, making it a promising solution for establishing trustworthy communication in IoT networks.