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

ENHANCING SECURITY IN IOT ROUTING: A LITERATURE REVIEW ON TRUST-BASED SECURED ROUTING SYSTEMS LEVERAGING MACHINE LEARNING ALGORITHMS

[1]R. Elango, [2]Dr. D. Maruthanayagam

[1]Research Scholar, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India

[2] Dean Cum Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.

Abstract: This literature review explores the implementation of trust-based secured routing systems in the Internet of Things (IoT) using machine learning techniques. It begins with an overview of the significance of secure routing in IoT networks and the importance of trust management. The review delves into existing trust-based routing approaches and discusses the role of machine learning in enhancing trust evaluation. **Various machine learning algorithms used for trust assessment are analyzed, highlighting their advantages and limitations**. The review concludes with an assessment of challenges, future directions, and potential advancements in the field, emphasizing the critical role of trust-based routing systems in enhancing IoT security.

Keywords: Internet of Things, IoT routing, trust management, machine learning, Quality of Service (QoS) and security.

I. INTRODUCTION

The Internet of Things (IoT) represents a paradigm shift in the way we interact with technology, connecting an ever-expanding array of devices to the internet to gather and exchange data autonomously. This interconnected network of devices spans (width) various domains, including smart homes, healthcare, transportation, and industrial automation, revolutionizing how we perceive and interact with our environment. **The significance of IoT lies in its transformative potential to enhance efficiency, productivity and convenience across industries**. By enabling seamless communication and data exchange between devices, IoT facilitates real-time monitoring, automation and decision-making, leading to improved resource utilization, cost savings and enhanced user experiences. However, the rapid proliferation of **IoT devices also introduces new challenges, particularly concerning security and privacy**. As the number of connected devices grows exponentially, so does the attack surface for malicious actors seeking to exploit vulnerabilities in IoT systems. Securing IoT networks against unauthorized access, data breaches and cyber-attacks has thus become a paramount concern for both industry stakeholders and policymakers [1]. One critical aspect of IoT security is the implementation of trust-based secured routing systems. Traditional routing protocols, such as the **Routing Protocol for Low-Power and Lossy Networks (RPL), are not inherently designed to address the unique security requirements of IoT** environments. Trust-based secured routing seeks to mitigate security risks by evaluating the trustworthiness of nodes and routes in IoT networks, thereby ensuring the integrity, confidentiality and availability of data transmission. **At the heart of trust-based secured routing lies the concept of trust management**, which involves assessing the reliability and reputation of individual nodes based on their behavior and interactions within the network. Trust metrics, reputation systems and trust establishment protocols play crucial roles in determining the trustworthiness of nodes and facilitating secure communication in IoT environments [2].

Machine learning (ML) techniques have emerged as powerful tools for enhancing the security and trustworthiness of IoT routing systems. By leveraging ML algorithms, IoT networks can analyze vast amounts of data to detect anomalies, predict malicious behavior and adaptively respond to emerging threats in real-time. ML-driven approaches enable dynamic trust assessment and routing decisions, thereby strengthening the resilience of IoT networks against evolving security threats. In this literature review, we delve into the intersection of trust-based secured routing, IoT security and machine learning [3]. We survey existing research, methodologies and challenges in this domain, aiming to provide insights into the state-of-the-art techniques for enhancing the security and trustworthiness of IoT routing systems. By exploring **the role of machine learning in augmenting trust management and mitigating security risks in IoT** environments, we seek to contribute to the ongoing discourse on securing the future of interconnected devices.

II. TRUST MANAGEMENT IN IOT

Trust management plays a pivotal (key) role in ensuring the security and reliability of IoT environments. In the context of IoT, where devices often operate in dynamic and heterogeneous networks, **trust management mechanisms are essential for establishing and maintaining trust relationships among participating entities**. Trust enables IoT devices to make informed decisions regarding data sharing, resource access, and collaboration, thereby enhancing the overall security posture of the ecosystem [4].

Effective trust management in IoT environments enables the following:

- ✓ **Secure Communication:** Trust-based mechanisms facilitate secure communication channels between IoT devices, ensuring that data exchanged between nodes remains confidential, integral and available.
- ✓ **Resource Management:** By assessing the trustworthiness of devices, IoT networks can efficiently allocate resources and prioritize tasks, optimizing network performance and energy consumption.
- ✓ **Access Control:** Trust management enables **fine-grained access control policies, allowing authorized devices to interact with sensitive data and services** while mitigating the risk of unauthorized access or malicious behavior.
- ✓ **Resilience to Attacks:** Trust-based approaches help IoT networks detect and mitigate various security threats, including malicious nodes, insider attacks and data tampering, thereby enhancing the overall resilience of the ecosystem.

Several trust management models and mechanisms have been proposed for IoT environments, each with its strengths, limitations and application domains. Some common trust management approaches include:

- ✓ **Certification-Based Trust:** This approach relies on **digital certificates and public-key infrastructure (PKI) to establish trust between IoT devices.** Devices are authenticated based on their cryptographic credentials, and trust is inferred from the validity and reputation of the certificates.
- ✓ **Reputation-Based Trust:** Reputation systems assess the **past behavior and interactions of IoT devices to determine their trustworthiness**. Devices with positive reputations are trusted more, while those with negative reputations may be subjected to additional scrutiny or restrictions.
- ✓ **Behavior-Based Trust:** Behavior-based trust models **analyze the real-time behavior of devices to assess their trustworthiness**. Machine learning algorithms can be employed to detect anomalies, deviations from expected behavior and potential security threats.
- ✓ **Trust Propagation:** Trust can be propagated through the network based on direct interactions between devices or through intermediary nodes. Trust propagation algorithms enable devices to make trust decisions based on the recommendations or endorsements of trusted peers.

Challenges Associated with Trust Establishment and Maintenance in IoT Networks:

Despite the importance of trust management, several challenges hinder its effective implementation in IoT environments:

- ✓ **Scalability:** IoT networks may consist of thousands or even millions of interconnected devices, making it challenging to scale trust management mechanisms to accommodate the dynamic nature of the ecosystem.
- ✓ **Heterogeneity:** IoT devices come in various forms, with diverse capabilities, communication protocols and security mechanisms. Trust management models must be adaptable to heterogeneous environments and interoperable across different device types.
- ✓ **Dynamicity:** IoT environments are characterized by dynamic network topologies, device mobility and changing environmental conditions. Trust management mechanisms must be agile and capable of adapting to evolving circumstances in real-time.
- ✓ **Resource Constraints:** Many IoT devices operate with limited computational resources, storage capacity and energy supply. Trust management solutions should be lightweight, energy-efficient and resource-aware to minimize overhead and ensure compatibility with constrained devices.
- ✓ **Security and Privacy:** Trust management mechanisms themselves are susceptible to security vulnerabilities and privacy breaches. Adversarial attacks, data manipulation and information leakage can undermine the integrity and effectiveness of trust-based systems.

III. MACHINE LEARNING TECHNIQUES FOR TRUST-BASED ROUTING

Machine learning (ML) techniques have shown significant promise in enhancing trust-based routing systems in IoT environments. **ML algorithms can analyze large volumes of data, identify patterns, and make predictions, enabling more accurate and adaptive trust assessment,** anomaly detection, and intrusion detection mechanisms [5][6]. Some common ML approaches used in trust-based routing systems include:

- ✓ **Supervised Learning:** Supervised learning algorithms, such as decision trees, support vector machines (SVM) and neural networks, can be trained on labeled datasets to classify nodes as trustworthy or untrustworthy based on features extracted from their behavior and interactions.
- ✓ **Unsupervised Learning:** Unsupervised learning techniques, including clustering algorithms and anomaly detection methods can identify abnormal patterns or deviations from expected behavior in IoT networks, flagging potential security threats or malicious activities.
- ✓ **Reinforcement Learning:** Reinforcement learning algorithms enable IoT devices to learn optimal routing strategies by interacting with their environment and receiving feedback based on the outcomes of their actions. This approach facilitates adaptive routing decisions based on the changing trustworthiness of nodes and network conditions.

Machine learning can enhance trust-based routing systems in IoT networks in several ways:

- ✓ **Trust Assessment: ML algorithms can analyze historical data on node behavior, communication patterns, and reliability metrics to infer (conclude) the trustworthiness** of individual nodes. By integrating machine learning with trust management frameworks, IoT networks can dynamically adjust trust scores based on real-time observations, improving the accuracy and responsiveness of trust assessment mechanisms.
- ✓ **Anomaly Detection:** ML-based anomaly detection techniques can identify abnormal behavior or deviations from normal patterns in IoT networks, signaling potential security threats or malicious activities. By leveraging anomaly detection algorithms, IoT routing systems can proactively detect and mitigate security breaches, minimizing the impact of cyber-attacks and data breaches.
- ✓ **Intrusion Detection: ML algorithms can learn to recognize patterns associated with specific types of cyber-attacks or intrusion attempts in IoT networks**. By analyzing network traffic, device interactions and system logs, ML-based intrusion detection systems can detect and classify

security incidents, enabling prompt response and remediation actions to mitigate potential risks.

Several case studies and examples demonstrate the effectiveness of ML-based approaches for securing IoT routing:

- ✓ **Behavior-Based Trust Management:** Researchers have developed ML models to analyze the behavior of IoT devices and assign trust scores based on their historical performance and interactions. These models adaptively update trust scores in response to changing network conditions and security threats, improving the resilience of IoT routing systems.
- ✓ **Anomaly Detection in IoT Networks: ML-based anomaly detection systems have been deployed to detect abnormal traffic patterns, unauthorized access attempts**, and other suspicious activities in IoT networks. By leveraging supervised and unsupervised learning techniques, these systems can identify anomalies indicative of security breaches or malicious behavior, enabling proactive threat mitigation.
- ✓ **Reinforcement Learning for Adaptive Routing:** Researchers have explored the use of reinforcement learning algorithms to optimize routing decisions in IoT networks. By learning from past experiences and environmental feedback, IoT devices can **dynamically adjust their routing strategies to avoid compromised nodes, congested paths,** or potential security risks, improving the overall reliability and efficiency of IoT routing.

IV. LITERATURE REVIEW

Muzammal et al.,(2022)[7] highlighted the vulnerability of the Routing Protocol for Low Power and Lossy Networks (RPL) in IoT networks, especially with the rising number of applications and devices. They proposed a Security, Mobility and Trust-based model (SMTrust) to address rank and Blackhole attacks, considering both static and mobile nodes. Their model integrates trust factors, including mobility-based metrics to enhance security without overburdening resource-constrained smart devices. Simulation results demonstrated SMTrust's superiority over existing methods, achieving a 46% increase in topology stability, 45% reduction in packet loss, and 35% throughput improvement with minimal power consumption rise. Given IoT's resource constraints, the study emphasizes the necessity of lightweight security mechanisms. Trust-based methods are preferred, yet existing literature inadequately addresses node mobility. The proposed SMTrust protocol selects trustworthy nodes as preferred parents, enhancing network security. Performance comparisons against other protocols showed SMTrust's superiority, particularly in scenarios involving static and mobile nodes. While SMTrust shows promising results in scenarios involving static and mobile nodes, further optimization is needed to fully address the dynamic nature of IoT environments. *One drawback of existing trust-based security solutions for IoT networks, including SMTrust, is the insufficient consideration of node mobility.* Future research should focus on enhancing mobility-aware trust computation and evaluating protocols for potential vulnerabilities such as colluding attacks.

Siddiqui et al.,(2023) [8] addressed trust assessment challenges in the Internet-of-Vehicles (IoV) by proposing a distributed trust management model. They emphasized the importance of precise parameter weighting and defining minimum trust thresholds to accurately identify dishonest vehicles. Utilizing an IoT dataset transformed into an IoV format, they computed influential parameters and formed feature matrices. Unsupervised learning was employed to establish ground truth, followed by supervised machine learning for classification. Their approach achieved perfect precision and recall using Subspace KNN for individual parametric scores and Subspace Discriminant for mean scores. FM2, considering averaged pairwise computations, outperformed FM1 in classification accuracy. Future work will explore additional trust parameters and dynamic attack models, along with the development of a purpose-built IoV simulator for generating large trust-based datasets. *One drawback is the reliance on predefined trust thresholds, potentially leading to delayed or inaccurate detection of dishonest vehicles. Additionally, the study's focus on specific trust parameters may overlook other influential factors affecting trust assessment in dynamic IoV environments.*

Kamran Ahmad Awan et al.,(2023) [9] proposed a machine learning-based trust management approach for IoT edge nodes to identify malicious behavior, particularly in healthcare applications. Their mechanism utilizes edge clouds for trust evaluation, ranking node trustworthiness and allowing only nodes meeting a threshold to participate. Extensive simulations demonstrate the effectiveness of the approach against various attacks, addressing the need for lightweight security and energy-efficient solutions in IoT environments, especially in healthcare. Future work may involve evaluating storage challenges and implementing a two-way trust management approach for hospitals. *Drawback is the reliance on predefined trust thresholds, potentially excluding nodes that may contribute positively but fall below the threshold. Additionally, the approach may require further evaluation for scalability and adaptability to diverse IoT environments beyond healthcare.*

Mohammad Sirajuddin et al.,(2021) [10] introduced a trust-based multipath routing protocol, TBSMR, for Mobile Ad Hoc Networks (MANETs) to enhance Quality of Service (QoS). TBSMR considers factors like congestion control, packet loss reduction and malicious node detection to improve overall performance. Simulation results in NS2 demonstrate its superiority over existing approaches, offering better performance in PDR, PLR, delay and throughput. Future work includes implementing security algorithms such as encryption, decryption and blockchain to enhance MANET security. *One potential drawback is the reliance on simulation results without real-world validation, which may not fully capture the complexities of MANET environments. Additionally, while TBSMR improves QoS, its effectiveness in highly dynamic and heterogeneous MANET scenarios remains to be explored.*

Tanzila Saba et al.,(2023) [11] proposed a smart optimization model for Internet of Agriculture Things (IoAT) to enhance agricultural sustainability. The model utilizes intelligent devices for data collection and transmission, leveraging machine learning for quality-aware decision-making. Additionally, blockchain-based security principles are integrated to ensure trusted communication and protect sensitive data. Simulation results validate the model's effectiveness in optimizing network parameters and improving data security. Future work will focus on evaluating intrusion detection performance and incorporating mobile cloud communication to enhance the model further. *Drawback is the reliance on simulation-based validation, which may not fully capture real-world complexities and scenarios. Additionally, while the proposed model improves data security and optimization, its* *scalability and adaptability to diverse agricultural environments remain to be explored.*

Geetha Pawar et al., (2023) [12] proposed an efficient trust inference model for ubiquitous computing, leveraging fine-tuned artificial neural networks (ANN) and machine learning (ML) for IoT attack prediction. Achieving 90.43% accuracy, their hybrid deep learning-based approach outperforms traditional classifiers like random forest, XGBoost, and SVM kernel. The study highlights the potential of the model to address trust, confidentiality and identification challenges in pervasive computing. Future research aims to extend the model's application to discriminatory recommendation engines and deployment on mobile devices for real-world validation. *Drawback is the reliance on a single dataset for model evaluation, which may limit the generalizability of results to diverse IoT attack scenarios. Additionally, while achieving high accuracy, the proposed model's complexity and resource requirements may pose challenges for implementation in resource-constrained IoT environments.*

Subhash Sagar et al.,(2020) [13] present a trust computational model for the Social Internet of Things (SIoT), leveraging machine learning for trust aggregation. In the Social Internet of Things (SIoT), devices function autonomously, intelligently exchanging information and discovering services through social relationships with their owners. Trust is pivotal in forming reliable connections between these objects, mitigating risks in decision-making processes. Their approach aims to identify trustworthy nodes by extracting individual trust features and employing k-means clustering for data labeling. Simulation results demonstrate the effectiveness of the proposed model in isolating trustworthy interactions. Future work will focus on incorporating experience as a trust attribute and exploring additional social features for improved trust determination in SIoT networks. *One potential drawback is the reliance on simulation-based evaluation, which may not fully capture real-world complexities and scenarios. Additionally, while the model shows promise, its effectiveness in dynamic and heterogeneous SIoT environments remains to be validated.*

Anup W. Burange et al.,(2023) [14] address routing challenges in Industrial Internet of Things (IIoT) applications, proposing a lightweight trust-based secured routing system to detect and isolate Rank, Sybil, and Wormhole attacks on RPL. Utilizing machine learning techniques, the system achieves high accuracy (98.59%) in attack detection and isolation, ensuring a secure routing environment. The system's hybrid trust evaluation, integrating direct, reputation, and experience trust, enhances its adaptability and efficiency. Validation within Contiki's Cooja simulator demonstrates promising results, with potential for future expansion to detect additional attack types and incorporate social attributes as trust metrics. *One limitation and also disadvantage is the reliance on simulation-based validation, which may not fully reflect real-world scenarios and complexities. Additionally, while the system effectively detects known attacks, its ability to adapt to novel attack types remains unexplored.*

Mohammad Khalid Imam Rahmani et al., (2022) [15] explore the Internet of Medical Things (IoMT), emphasizing its integration with healthcare systems via the internet. While cloud computing in IoMT enhances scalability and resource utilization, security breaches remain a concern. This study reviews trust challenges in cloud computing and evaluates blockchain-based trust management frameworks to address them. Through a systematic review, ten solutions categorized into decentralization and security are identified, addressing challenges such as centralization, overhead, trust evidence, adaptiveness and accuracy. The study underscores the role of blockchain technology in managing trust in cloud systems and cloud-based IoMT, offering insights for future research in the field. *One limitation (drawback) is the potential bias in the manual coding process, which may affect the categorization of quotations and solutions. Additionally, the reliance on keyword analysis could overlook relevant articles that do not contain specific keywords.*

Salunkhe Madhav Jagannath et al., (2023) [16] addressed security concerns in IoT systems by integrating machine learning (IML) and deep learning algorithms. Their method employs attack models to detect threats, utilizing network traffic data for training features. By focusing on Convolutional Neural Networks (CNN) for classification, their approach achieves high accuracy (~0.9976) with low execution time (1.30 sec) and improved recall and G-mean values. Their study highlights the effectiveness of ML-DL techniques in mitigating IoT threats, particularly through CNN-based intrusion detection and classification. Comparison with traditional methods demonstrates the superior performance of their approach, emphasizing its novelty and potential for enhancing IoT security. *The research lacks a detailed comparison with state-of-the-art methods, potentially limiting insight into the relative performance of the proposed ML-DL technique. Additionally, it could not benefit from a discussion on the scalability and generalizability of the proposed approach to diverse IoT environments and attack scenarios.*

Amr M. T. et al., (2022) [17] present a hybrid strategy for trust computation in IoT scenarios, integrating social similarity and machine learning techniques. Their approach incorporates features like user centrality, popularity, and interactions, with a focus on highly trusted parties. Dynamic trust aggregation based on users' social behavior is proposed, facilitated by a cloud-based architecture. Experimental results demonstrate superior performance compared to existing methods, with machine learning slightly outperforming traditional computational models. The study highlights the effectiveness of social similarity and trusted parties in mitigating fraudulent activities and proposes dynamic aggregation for real-time datasets. Future work aims to address opportunistic attacks and implement the approach in real-world settings. *The study lacks detailed the implementation of the proposed hybrid strategy for trust computation in IoT scenarios. There is limited discussion on the scalability and adaptability of the approach to different network sizes and dynamics.*

Wei Ma et al., (2021) [18] present to the escalating security threats posed by malicious IoT devices, this research introduces a machine learning-driven trust evaluation approach. By leveraging deep learning algorithms, specifically LSTM neural networks, the method aggregates network QoS properties to construct a behavioral model for individual IoT devices. This model, trained on device-specific network flows, predicts future behaviors, facilitating the quantification of trust through continuous numerical values derived from the similarity between predicted and observed behaviors. Experimental validation confirms the effectiveness of the proposed approach in identifying abnormal devices and supporting decision-making processes in IoT networks. *The proposed trust evaluation method for IoT devices relies heavily on deep* *learning algorithms, potentially requiring significant computational resources and expertise, which could limit its applicability in resource-constrained environments. Additionally, the method's effectiveness may be influenced by the quality and representativeness of the training data, leading to potential biases or inaccuracies in trust assessments.*

R. Mohan Das et al.,(2023) [19] introduce a novel Multi-hop Convolutional Neural Network with an attention mechanism (MH-CNN-AM) to enhance the detection of fraudulent nodes in SIoT networks. They assess its performance using metrics like accuracy, precision, recall, F1-score, and MAE, comparing it with existing methodologies. As SIoT networks expand, the emergence of new attacks and hazards necessitates scalable solutions, making MH-CNN-AM a promising approach. However, integrating high-order neighbor-node interactions poses computational challenges. In the realm of the 'Social Internet of Things' (SIoT), concerns over privacy and security hinder its widespread adoption. Existing approaches lack the ability to effectively identify fraudulent nodes or discern various types of attacks. To address this, they propose a novel Multi-hop Convolutional Neural Network with an attention mechanism (MH-CNN-AM) specifically designed to detect hostile nodes and enhance network security. However, integrating high-order neighbor-node interactions into the model presents computational challenges. *The disadvantage of proposed Multi-hop Convolutional Neural Network with an attention mechanism may not encounter computational challenges in learning high-order neighbor-node interactions, potentially limiting its scalability and efficiency.*

Kunkun Rui et al.,(2023) [20] proposed SRAIOT, a hierarchical algorithm for enhancing Secure Routing in IoT networks, leveraging SDN for network management. Controller nodes in each subnet monitor traffic patterns using an ensemble learning model to detect attacks, improving routing efficiency and attack detection. However, addressing security issues inherent in SDN communication channels and managing the computational load of the ensemble system are potential areas for further research. SRAIOT enhances Secure Routing in IoT networks by leveraging a hierarchical structure and SDN technology, resulting in improved routing efficiency and effective attack detection. *The drawback is reliance on SDN for security introduces potential vulnerabilities, such as man-in-the-middle attacks due to security issues in the communication channel. Additionally, the ensemble learning model could not used for attack detection may increase computational load, requiring optimization for efficiency.*

Anuoluwapo A et al.,(2021) [21] address these challenges of future Internet of Things (IoT) will rely on lightweight computing platforms offering individual micro services, leading to complex service compositions with increased security risks. A novel model called SC-TRUST is proposed, focusing on transparent trust composition and decomposition. SC-TRUST improves service quality and mitigates trust-related attacks, enhancing both efficiency and security in IoT service compositions. SC-TRUST improves service quality and mitigates trust-related attacks, enhancing both efficiency and security in IoT service compositions. *However, this study does not consider the impact of constraints such as price and energy on service composition, which warrants further investigation in future research.*

Yara Alghofaili et al.,(2022) [22] proposed a trust management model for IoT devices and services based on the Simple Multi-Attribute Rating Technique (SMART) and the Long Short-Term Memory (LSTM) algorithm. SMART calculates trust values, while LSTM detects behavioral changes based on a trust threshold. In various aspects of life, including transportation, healthcare and education, the Internet of Things (IoT) technology has recently gained prominence. It enables smart services, allowing devices to provide suitable services to users anytime and anywhere by interacting with the physical world intelligently. However, this technological advancement has led to an increase in the number and complexity of attacks, posing trust challenges to IoT smart services. Although trust management techniques have been employed to address these challenges, they often face limitations in handling large amounts of data and dynamically changing behaviors. The effectiveness of the model is evaluated using accuracy, loss rate, precision, recall and F-measure on different data samples of varying sizes. The proposed model demonstrates superior performance compared to existing machine learning and deep learning models, achieving 89.87% accuracy and 89.76% F-measure with 100 iterations. This suggests that the model is effective in addressing trust-related challenges in the IoT domain. In future research, additional features, such as energy consumption of IoT devices, will be considered to enhance trust calculation. The proposed trust management model leverages the Simple Multi-Attribute Rating Technique (SMART) and the Long Short-Term Memory (LSTM) algorithm, which are effective in calculating trust values and detecting behavioral changes with high accuracy. Through extensive evaluation, the model demonstrates superior performance compared to existing machine learning and deep learning approaches, achieving impressive accuracy and F-measure scores, thereby enhancing trust-related aspects of IoT services. *One potential drawback is the computational complexity associated with the LSTM algorithm, which may require significant computational resources, especially when dealing with large-scale IoT deployments or real-time data processing. While the proposed model shows promising results, its effectiveness may still be influenced by various factors such as the quality and diversity of the data samples used for training and testing, as well as the specific characteristics of the IoT environment in which it is deployed.*

DooHo Keum et al.,(2022) [23] address the challenge of ensuring trustworthy and timely routing in mission-critical wireless sensor networks (MC-WSNs), vital for transmitting mission-critical data reliably amidst potential cyber-attacks. This proposed trust-based routing protocol employs Q-learning to discern attacks and optimize network performance, ensuring prompt threat detection and secure data transmission. By prioritizing trustworthiness, QoS and energy efficiency, their distributed transmission technology, MC-TIRP, caters to resource-constrained MC-WSN environments, exhibiting enhanced performance metrics such as packet delivery rates, throughput, survivability and delay compared to alternative methods. While promising, future research avenues may explore further improvements in trust evaluation techniques to bolster the security of mission-critical data. The proposed trust-based routing protocol enhances the reliability and trustworthiness of mission-critical data transmission in wireless sensor networks. By employing Q-learning to detect and mitigate cyber threats, the protocol ensures prompt threat detection and secure communication, vital for decision-making and secure data transfer. *While this method implementing trust-*

based routing protocols may introduce additional computational overhead and complexity to the network nodes, potentially impacting resource-constrained devices. While the protocol exhibits enhanced performance metrics compared to alternative methods, further research is needed to optimize its efficiency and scalability in large-scale sensor networks.

Syeda Mariam Muzammal et al.,(2022) [24] introduces the Security, Mobility and Trust-based model (SMTrust), tailored to combat Rank and Blackhole attacks in RPL-based IoT networks. To address these gaps, this IoT networks, the prevailing Routing Protocol for Low Power and Lossy Networks (RPL) faces increasing vulnerability to routing attacks, necessitating robust security measures. While existing solutions, including trust-based approaches, show promise, they often overlook nodes' mobility and lack evaluation for dynamic scenarios. By integrating carefully selected trust factors, including mobility-based metrics, SMTrust demonstrates superior performance compared to existing methods, enhancing topology stability, reducing packet loss, and increasing throughput while maintaining minimal power consumption. SMTrust offers a comprehensive approach to securing RPL-based IoT networks by integrating security, mobility, and trust considerations. The proposed model outperforms existing trust-based methods, achieving notable improvements in topology stability, packet loss reduction and throughput enhancement, with minimal impact on power consumption. *Its remains there was one problem, even though its advancements, SMTrust may necessitate and further optimization to address power consumption concerns and evaluate its effectiveness need against additional threats, such as end-to-end delay and colluding attacks, in real-world implementations.*

Yingxun Wang et al.,(2024) [25] present a significant contribution to the field with their proposal of MESMERIC, a machine learning-based trust management mechanism for Internet of Vehicles (IoV) networks. MESMERIC integrates various trust attributes and contextual factors to effectively evaluate and distinguish trustworthy vehicles from untrustworthy ones, thereby enhancing the reliability of safety-critical information exchange within IoV networks. Evaluation results showcase MESMERIC's superiority over existing trust management mechanisms, highlighting its potential to bolster network security and improve vehicle-to-vehicle communication efficiency. MESMERIC introduces an advanced trust management mechanism for IoV networks, leveraging machine learning to comprehensively evaluate trustworthiness based on diverse trust attributes and contextual factors.Extensive evaluation demonstrates MESMERIC's superior performance compared to existing trust management mechanisms, promising more dependable vehicle-to-vehicle communication and heightened overall network security. *In the meanwhile, some drawbacks overcome with in the future research must have need some avenues investigating dynamic trust-related attacks and devising resilient trust models tailored for IoV networks. Additionally, efforts to mitigate subjectivity in trust aggregation through intelligent weighting-based approaches could further fortify trust management in IoV environments.*

Sahraoui Dhelim et al.,(2023) [26] introduce Trust2Vec, a novel trust management system designed specifically for large-scale Internet of Things (IoT) networks. Unlike existing systems tailored for small-scale trust attacks, Trust2Vec addresses the challenge of large-scale trust attacks perpetrated by numerous malicious devices. Leveraging a random-walk network exploration algorithm, Trust2Vec computes trust network embeddings to analyze latent trust relationships within the network, even in the absence of direct trust ratings between malicious devices. Additionally, Trust2Vec employs a network embeddings community detection algorithm to identify and block communities of malicious nodes, effectively mitigating large-scale attacks such as self-promotion and bad-mouthing. Simulation results demonstrate Trust2Vec's effectiveness, achieving up to a 90% mitigation rate across various network scenarios. Trust2Vec offers a tailored solution for managing trust relationships in large-scale IoT systems, addressing the limitations of existing trust frameworks designed for small-scale networks. Through sophisticated algorithms, Trust2Vec effectively identifies and mitigates large-scale trust attacks, enhancing the security and reliability of IoT networks. *Drawback is improvements may include customization of Trust2Vec for specific IoT applications, particularly in dynamic environments like vehicular networks, and extension to manage trust in virtual network entities via software-defined networking. Further enhancements could involve expanding Trust2Vec's scope to include trust management of data entities, in addition to network devices, to provide comprehensive security coverage in IoT environments.*

Raghavendra et al.,(2022)[27] underscore the pivotal role of the Internet of Things (IoT) in enhancing human life, with sensors serving as vital components for environmental detection within IoT ecosystems. As IoT adoption surges, driven by the proliferation of internet-connected devices leveraging IPv6, the demand for efficient routing protocols intensifies. While traditional protocols like OSPF and RIP are unsuitable for Low-Power and Lossy Network (LLN) Routers in IoT due to resource constraints, the Routing Protocol for Low-power and Lossy Networks (RPL) emerges as a promising solution. However, RPL remains susceptible to various attacks such as decreased rank, black hole, and sinkhole attacks. To address these vulnerabilities, the authors propose an Intrusion Detection System (IDS) based on machine learning (ML) algorithms tailored for IoT environments. Their approach integrates genetic recursive feature selection and fuzzy k-nearest neighbor classification algorithms to enhance attack detection accuracy while minimizing false positives. Through extensive performance evaluations, including precision, recall, and F1-score comparisons with existing works, the proposed IDS demonstrates superior efficacy in detecting RPL attacks. Moving forward, the authors advocate for further advancements, particularly in leveraging deep learning techniques to enhance attack detection accuracy, encompassing both known and unknown threats in IoT networks. The proposed Intrusion Detection System (IDS) leverages machine learning algorithms to enhance attack detection accuracy in IoT networks, improving overall network security. *Drawback is while implementing deep learning approaches for attack detection may introduce computational complexities, potentially impacting real-time performance in IoT environments.*

Ioulianou et al.,(2022) [28] address the critical security challenges presented by routing attacks in Internet of Things (IoT) networks, particularly those employing the Routing Protocol for Low-power and Lossy Networks (RPL). These attacks, including rank and blackhole attacks, exploit vulnerabilities in RPL, resulting in disruptive denial-of-service (DoS) incidents. To counter these threats, the authors propose a pioneering security framework for RPL-based IoT networks, termed SRF-IoT. This framework integrates a trust-based mechanism aimed at identifying and isolating malicious actors, alongside an external Intrusion Detection System (IDS). Both SRF-IoT and IDS are implemented within the Contiki-NG operating system. Through comprehensive simulations utilizing the Whitefield framework, which combines Contiki-NG and NS-3 simulators, the authors assess the efficacy of their proposed framework. These results underscore the effectiveness and potential of SRF-IoT in fortifying IoT networks against routing attacks, leveraging a synergistic blend of trust-based and IDS-based strategies, while minimizing disruptions to existing smart devices. Looking ahead, the authors envision expanding the detection capabilities of SRF-IDS to encompass a broader spectrum of attack types, such as sinkhole attacks, and exploring the integration of machine learning models for the detection of unknown threats. *One drawback of the proposed SRF-IoT framework is its reliance on external intrusion detection systems, which may introduce additional complexity and dependencies into the network architecture. Additionally, while SRF-IoT effectively mitigates known routing attacks, its ability to detect and respond to novel or unknown threats remains an area for further improvement.*

F. Zahra et al.,(2022) [29] highlight the security challenges posed by the Internet of Things (IoT), particularly in the context of routing attacks targeting the Routing Protocol for Low-power and Lossy Networks (RPL). To address this, they propose a lightweight multiclass classification-based attack detection model called MC-MLGBM. This model leverages a novel dataset generated using the Cooja simulator and optimized feature selection techniques. Through extensive experiments, including evaluation metrics such as accuracy, precision, and recall, the proposed model demonstrates promising results in detecting RPL-specific rank attacks and sensor-network-inherited wormhole attacks. However, the study acknowledges the need for further diversification of attack data in the dataset and suggests future research directions to address this limitation and enhance the model's effectiveness in detecting a broader range of attacks. *The study acknowledges some difficulties of the need for further diversification of attack data in the dataset, which may limit the model's applicability to a broader range of attacks. Additionally, while the proposed model shows promising results, further developments are required to enhance its effectiveness in detecting various types of routing attacks beyond rank attacks and wormhole attacks.*

Arshad et al.,(2022)[30] present a novel Trust-Based Hybrid Cooperative (THC-RPL) protocol to address internal attacks in RPL-based IoT networks. By leveraging trust values calculated based on observed behavior, THC-RPL detects malicious Sybil nodes efficiently. Compared to existing methods, THC-RPL demonstrates superior performance, detecting more attacks while maintaining a packet loss ratio of 15-25% and achieving energy savings of 40% per node with a 50% increase in network lifetime. The protocol involves node registration and global trust calculation at the root node, enabling the isolation of malicious nodes and the participation of trusted nodes in routing. Evaluation metrics indicate THC-RPL's effectiveness, surpassing state-of-the-art solutions. Future work aims to validate THC-RPL in real testbed configurations. *THC-RPL may face challenges in scaling to larger networks due to increased computational overhead for trust calculation and propagation. Additionally, its reliance on centralized trust evaluation at the root node could introduce single points of failure and scalability issues in highly dynamic environments.*

Belavagi et al.,(2023)[31] explore the rising applications of wireless sensor networks, particularly in areas like environmental monitoring and agriculture, using the IPv6-based Routing Protocol for Low power and Lossy networks (RPL). Due to limited resources and the placement of sensor nodes in remote areas, security becomes paramount, prompting the development of an Intrusion Detection System (IDS). Their proposed IDS model leverages machine learning techniques like Artificial Neural Networks, Logistic Regression, Support Vector Machine, and Random Forest to dynamically identify multiple intrusions while optimizing energy consumption. The framework, starting from data generation using the Cooja simulator to rule generation based on supervised machine learning models, particularly highlights the effectiveness of the Random Forest model in generating rules. Deploying the rule generation process at the base station minimizes energy consumption by IDS-agent nodes, with IDS-agent clusters communicating any detected malicious activity to the base station. Future enhancements could involve expanding the range of attacks considered and evaluating IDS performance using different intrusion detection techniques. *Here, the Existing intrusion detection mechanisms are insufficient in dynamically identifying multiple intrusions and consume excessive energy, potentially degrading network performance.*

V.CONCLUSION

In conclusion, this **literature review underscores the importance of trust-based secured routing systems in ensuring the security and reliability of IoT networks**. Through the exploration of existing literature, we have identified various trust-based routing protocols and algorithms as well as the role of machine learning in enhancing trust evaluation. **Case studies and applications have illustrated the practical implementations and benefits of trust-based routing** systems across different IoT domains. However, challenges such as scalability, robustness and adaptability remain, pointing towards the need for further research and innovation in this area. Moving forward, advancements in machine learning techniques and the integration of novel methodologies hold the potential to address these challenges and **further improve the effectiveness of trust-based secured routing in IoT networks, ultimately contributing to the advancement of IoT security.**

Challenges, future directions and potential advancements:

In the rapidly evolving landscape of the Internet of Things (IoT), trust-based secured routing systems play a pivotal role in ensuring the integrity and security of interconnected devices and networks. However, these systems face several significant challenges that must be addressed to realize their full potential. One of the primary challenges is scalability, as **IoT networks continue to grow in size and complexity**, **requiring trust mechanisms that can efficiently handle a large number of devices** and dynamic network conditions. **Additionally, ensuring the robustness of trust mechanisms against various attacks** and adversarial behaviors is critical for maintaining the security posture of IoT networks. Another challenge lies in adapting trust-based routing systems to **dynamic network conditions, including changes in topology, mobility patterns and environmental factors**.

Moreover, resource constraints pose a significant obstacle, as IoT devices often have **limited computational resources, memory, and energy, making it challenging to implement** complex trust evaluation algorithms. Privacy concerns also loom large, as trust management involves the exchange of sensitive information among devices, necessitating mechanisms to protect user data and privacy. **Addressing these challenges requires innovative solutions and future directions for research and development**. Looking ahead, several promising avenues for advancement emerge. Integration of blockchain technology holds potential for enhancing the security and transparency of trust-based routing systems by providing tamper-proof and decentralized transaction ledgers. Leveraging edge computing capabilities can enable distributed trust evaluation closer to IoT devices, reducing latency and enhancing scalability. Federated learning approaches offer opportunities for collaborative trust evaluation without centralized data aggregation, preserving privacy and scalability. Furthermore, advancements in behavioral analysis techniques, such as **anomaly detection and machine learning-based behavior prediction, can improve the accuracy of trust assessment in IoT networks**.

Standardization efforts are also crucial, as establishing standardized protocols and frameworks for trust management in IoT can facilitate interoperability, promote adoption and enhance overall security. Hybrid trust models that combine multiple trust evaluation techniques, adaptive trust thresholds that dynamically adjust based on contextual factors, and explainable AI techniques for transparency and interpretability in trust decision-making processes are potential advancements that can enhance the resilience and trustworthiness of IoT networks. Moreover, extending trust management beyond individual IoT domains to enable cross-domain trust establishment and collaboration as well as integrating human-in-the-loop trust mechanisms, can further enhance the security, resilience and user acceptance of IoT devices and services. **Overall, addressing these challenges and pursuing these future directions and potential advancements** will be instrumental in advancing the field of trust-based secured routing systems in the Internet of Things.

VI.REFERENCES

[1]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[2]. Y. Sun, H. Song, A. Jara, S. Bie, and M. Suzuki, "Internet of things and big data analytics for smart and connected communities," IEEE Access, vol. 4, pp. 766-773, 2016.

[3]. R. Ma, Y. Zhang, and L. Su, "A Survey on Trust Management for Internet of Things," in 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1135-1140.

[4]. F. Karim, M. Othman, and N. Mohamed, "Trust management in Internet of Things: A systematic review," Journal of Network and Computer Applications, vol. 101, pp. 15-29, 2018.

[5]. K. Srinivasan and L. L. L. Pollock, "A Learning Approach to Trusted Information Sharing," in 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 2017, pp. 3620-3629. DOI: 10.1109/BigData.2017.8258309.

[6]. Y. Liu, J. Li, X. Zhou, and W. Zhuang, "A Data Trustworthiness Evaluation Model Based on Machine Learning," in 2018 IEEE Trustcom/BigDataSE/ISPA, New York, NY, USA, 2018, pp. 928-935. DOI: 10.1109/TrustCom/BigDataSE/ISPA.2018.00146.

[7]. Muzammal, S.M.; Murugesan, R.K.; Jhanjhi, N.Z.; Humayun, M.; Ibrahim, A.O.; Abdelmaboud, A. A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things. Sensors 2022, 22, 7052. https://doi.org/10.3390/s22187052

[8]. Siddiqui, S.A.;Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. Towards a Machine Learning Driven Trust Management Heuristic for the Internet of Vehicles. Sensors 2023, 23, 2325. https://doi.org/10.3390/s23042325

[9]. Awan, K.A.; Ud Din, I.; Almogren, A.; Khattak, H.A.; Rodrigues, J.J.P.C. EdgeTrust: Lightweight Data-Centric Trust Management Approach for IoT-Based Healthcare 4.0. Electronics 2023, 12, 140. https://doi.org/10.3390/electronics12010140

[10]. Mohammad Sirajuddin, Ch. Rupa , Celestine Iwendi , and Cresantus Biamba ,"TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network", Hindawi, Security and Communication Networks, Volume 2021, Article ID 5521713, 9 pages, https://doi.org/10.1155/2021/5521713

[11]. Tanzila Saba , Amjad Rehman , Khalid Haseeb , Saeed Ali Bahaj , Jaime Lloret , " Trust-based decentralized blockchain system with machine learning using Internet of agriculture things", Computers and Electrical Engineering 108 (2023), 108674, https://doi.org/10.1016/j.compeleceng.2023.108674

[12]. Geetha Pawar, Jayashree Agarkhed,"Efficient Trust Inference Model for Pervasive Computing Based on Hybrid Deep Learning",International Journal of Intelligent Systems and Applications in Engineering IJISAE, 2023, 11(2), 170–179

[13]. S. Sagar, A. Mahmood, Q. Z. Sheng and W. E. Zhang, "Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach," *ICC 2020 - IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148767.

[14]. Anup W. Burange, Dr. Vaishali M. Deshmukh," Securing IoT Attacks: A Machine Learning Approach for Developing Lightweight Trust-Based Intrusion Detection System", International Journal on Recent and Innovation Trends in Computing and Communication", ISSN: 2321-8169 Volume: 11 Issue: 7June 2023, DOI: https://doi.org/10.17762/ijritcc.v11i7.7788

[15]. Mohammad Khalid Imam Rahmani , Mohammed Shuaib , Shadab Alam, Shams Tabrez Siddiqui, Sadaf Ahmad, Surbhi Bhatia and Arwa Mashat. "Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT):A Systematic Review", Hindawi, Computational Intelligence and Neuroscience, Volume 2022, Article ID 9766844, 14 pages, https://doi.org/10.1155/2022/9766844

[16]. Jagannath SM, Mohite RB, Gupta MK, Lamba OS (2023) Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems . Indian Journal of Science and Technology 16(9): 640-647. https://doi.org/10.17485/IJST/v16i9.99

[17]. Amr M. T. Ali-EldinID, A hybrid trust computing approach for IoT using social similarity and machine learning, Computing approach for IoT using social similarity and machine learning. PLoS

ONE 17(7): 0265658, 2022, https://doi.org/10.1371/journal.pone.0265658

[18]. Wei Ma, Xing Wang, Mingsheng Hu, And Qinglei Zhou,"Machine Learning Empowered Trust Evaluation Method for IoT Devices, Volume 9, 2021 65066-65077,IEEE Access, *DOI://10.1109/ACCESS.2021.3076118*

[19]. R. Mohan Das,U. Arun Kumar, S. Gopinath,V. Gomathy, N. A. Natraj, N. K. Anushkannan and Adhavan Balashanmugham,"A novel deep learning-based approach for detecting attacks in social IoT",Springer, Soft Computing, April 2023, https://doi.org/10.1007/s00500-023-08389-1

[20]. Kunkun Rui , Hongzhi Pan & Sheng Shu ,"Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques", Scientific Reports, (2023) 13:18003, https://doi.org/10.1038/s41598-023-44764-6

[21]. Anuoluwapo A. Adewuyi, Hui Cheng, Qi Shi, Jiannong Cao, Xingwei Wang, and Bo Zhou,"SC-TRUST: A Dynamic Model for Trustworthy Service Composition in the Internet of Things", IEEE Internet Of Things Journal, 2327-4662 (c) 2021.

[22]. Yara Alghofaili and Murad A. Rassam,A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique, Sensors 2022, 22, 634., https://doi.org/10.3390/s22020634

[23]. DooHo Keum and Young-Bae Ko, Trust-Based Intelligent Routing Protocol with Q-Learning for Mission-CriticalWireless Sensor Networks, Sensors 2022, 22, 3975. https://doi.org/10.3390/s22113975

[24]. Syeda Mariam Muzammal, Raja Kumar Murugesan, Noor Zaman Jhanjhi, Mamoona Humayun,Ashraf Osman Ibrahim and Abdelzahir Abdelmaboud, A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things, Sensors 2022, 22, 7052. https://doi.org/10.3390/s22187052

[25]. Wang, Y.; Mahmood, A.; Sabri, M.F.M.; Zen, H.; Kho, L.C. MESMERIC: Machine Learning-Based Trust Management Mechanism for the Internet of Vehicles. Sensors 2024, 24, 863. https://doi.org/10.3390/s24030863

[26]. Dhelim, S., Aung, N., Ning, H., Chen, L., & Lakas, A. (2023). Trust2Vec: Large-Scale IoT Trust Management System based on Signed Network Embeddings. IEEE Internet of Things, 10(1), 1-10. https://doi.org/10.1109/JIOT.2022.3201772

[27]. Raghavendra.T, Anand M, Selvi Ma, Thangaramya Kc, Santhosh Kumar,"An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things",4th International Conference on Innovative Data Communication Technology and Application,Elsevier,Procedia Computer Science 215 (2022) 61–70, https://doi.org/10.1016/j.procs.2022.12.007

[28]. Ioulianou, P.P.; Vassilakis,V.G.; Shahandashti, S.F. ATrust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks. Journal of Cybersecurity and Privacy, 2022, 2, 124–153. ISSN 2624-800X https://doi.org/10.3390/jcp2010009

[29]. Zahra, F.; Jhanjhi, N.Z.; Brohi, S.N.; Khan, N.A.; Masud, M.; AlZain, M.A. Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning. Sensors **2022**, 22, 6765. https://doi.org/10.3390/s22186765

[30]. Arshad D, Asim M, Tariq N, Baker T, Tawfik H, Al-Jumeily OBE D (2022),"THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack". PLoS ONE 17(7): e0271277. https://doi.org/10.1371/journal.pone.0271277

[31]. Manjula C Belavagi and Balachandra Muniyal,"Intrusion Detection Using Rule Based Approach in RPL Networks",IAENG International Journal of Computer Science, 50:3, IJCS_50_3_21,Volume 50, Issue 3: September 2023

ABOUT THE AUTHORS

R.Elango received his **M.Phil** degree from Thiruvalluvar University, Vellore in the year 2011. He received his **MCA** degree from Anna University, Chennai in the year 2010. He is pursuing his **Ph.D** degree (Part Time) at Sri Vijay Vidyalaya College of Arts and Science, Nallampalli, Dharmapuri, Tamil Nadu, India. He is working as a Guest Lecturer in the Department of Computer Science at Government Arts College for Men, Krishnagiri. His current research interest includes Internet of Things, Computer Networks, Cloud Computing and Network Security.

Dr.D.Maruthanayagam received his **Ph.D** Degree from Manonmaniam Sundaranar University, Tirunelveli in the year 2014. He received his **M.Phil** Degree from Bharathidasan University, Trichy in the year 2005. He received his **M.C.A** Degree from Madras University, Chennai in the year 2000. He is working as **Dean cum Professor**, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. He has above **23 years** of experience in academic field. He has published **8 books**, more than **65 papers** in International Journals and **35 papers** in National & International Conferences so far. His areas of interest include Computer Networks, Grid Computing, Cloud Computing and Mobile Computing.